JABATAN PERDANA MENTERI
JABATAN PERKHIDMATAN AWAM

POLISI KESELAMATAN SIBER

VERSI 2.0

ISI KANDUNGAN

SEJARAH POLISI KESELAMATAN SIBER

VERSI	KELULUSAN	TARIKH KUAT KUASA
1.0	JPICT	18 DISEMBER 2020
1.1	JPICT	16 NOVEMBER 2021
1.2	JPICT	14 DISEMBER 2022
1.3	JPICT	7 DISEMBER 2023
2.0	JPICT	7 NOVEMBER 2024

PENGENALAN

Polisi Keselamatan Siber (PKS) Jabatan Perkhidmatan Awam (JPA) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi semasa menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Polisi ini juga menerangkan kepada pengguna mengenai tanggungjawab dan peranan pengguna dalam melindungi aset ICT JPA. Polisi Keselamatan Siber (PKS) JPA disediakan berpandu kepada piawaian antarabangsa iaitu ISO/IEC 27001:2022 *Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems.*

OBJEKTIF

Objektif utama PKS adalah seperti yang berikut:

1. Memastikan kelancaran operasi jabatan yang berlandaskan ICT dengan mencegah serta meminimumkan risiko kerosakan atau kemusnahan aset ICT jabatan;

2. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, tidak boleh disangkal, ketersediaan dan kesahihan;

3. Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan aset ICT; dan

4. Meningkatkan tahap kesedaran keselamatan ICT kepada para kakitangan, pengguna dan Pihak Luaran.

PERNYATAAN POLISI

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Keselamatan ialah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.

Keselamatan ICT adalah bermaksud keadaan bagi segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan. Terdapat empat (4) komponen asas keselamatan IT, iaitu:

1. Melindungi maklumat rasmi JPA dari capaian tanpa kuasa yang sah;
2. Menjamin setiap maklumat adalah tepat, lengkap dan terkini;
3. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
4. Memastikan akses hanya kepada pengguna yang sah dan penerimaan maklumat daripada sumber yang boleh dipercayai.

PKS JPA merangkumi perlindungan ke atas semua bentuk maklumat digital dan bukan digital bertujuan untuk menjamin keselamatan maklumat tersebut dan ketersediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti yang berikut:

1. Kerahsiaan – maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan akses tanpa kebenaran.
2. Integriti – data dan maklumat hendaklah tepat, lengkap dan terkini. Ia hanya boleh diubah dengan cara yang dibenarkan sahaja.
3. Tidak boleh disangkal – punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal.
4. Kesahihan – data dan maklumat hendaklah dijamin kesahihannya.
5. Ketersediaan – data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain itu, analisis tahap risiko aset ICT dikenal pasti, seterusnya mengambil tindakan untuk merancang dan mengawal risiko berkenaan.

SKOP

Sistem ICT JPA terdiri daripada organisasi, manusia, perisian, peralatan, telekomunikasi, kemudahan ICT, data dan maklumat. JPA telah menetapkan keperluan-keperluan asas keselamatan seperti yang berikut:

1. Data dan maklumat termasuk *hardcopy* dan *softcopy* hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan dengan cara yang boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti.

2. Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan melindungi kepentingan JPA.

PKS JPA merangkumi perlindungan ke atas semua bentuk maklumat ICT kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar dan yang dibuat salinan. Ini akan dilakukan melalui penubuhan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

1. Data dan Maklumat

   Semua data dan maklumat elektronik dan bercetak yang disimpan atau digunakan di pelbagai media termasuk prosedur, manual pengguna, sistem dokumentasi, rekod, pangkalan data dan lain-lain;

2. Peralatan ICT

   Semua peralatan komputer seperti komputer peribadi, komputer riba, pencetak, media storan, server, *firewall*, peralatan multimedia & komunikasi dan alat sokongan yang lain;

3. Perisian

   Semua jenis perisian yang digunakan untuk mengendali, memproses, menyimpan dan menghantar data atau maklumat. Ini termasuklah sistem aplikasi seperti HRMIS, eSILA, EPSA dan perisian sistem seperti Windows, LINUX dan perisian utiliti, perisian komunikasi, sistem pengurusan pangkalan data, kod sumber dan lain-lain;

4. Perkhidmatan

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi- fungsinya.

Contoh:

i. perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. sistem halangan akses seperti sistem kad akses; dan
iii. perkhidmatan sokongan seperti kemudahan elektrik, pendingin hawa, sistem pencegah kebakaran dan lain-lain.

5. Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian bagi mencapai misi dan objektif; dan

6. Persekitaran Fizikal

Persekitaran fizikal yang merujuk kepada lokasi fizikal yang menempatkan perkara 1 - 5 di atas.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada PKS JPA adalah seperti yang berikut:

1. Akses Atas Dasar Perlu Mengetahui

   Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar perlu mengetahui sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut.

2. Hak Akses Minimum

   Hak akses kepada pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/ atau melihat sahaja. Kelulusan khas diperlukan untuk membolehkan pengguna mencipta, menyimpan, mengemas kini, mengubah dan menghapuskan sesuatu data atau maklumat.

3. Kebertanggungjawaban atau Akauntabiliti

   Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Bagi menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesahkan bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

4. Pengasingan

   Tugas mencipta, menghapus, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan (*unauthorized access*) serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasikan. Pengasingan juga merangkumi data, operasi, pangkalan data dan rangkaian.

5. Pengauditan

   Tujuan aktiviti ini ialah untuk mengenal pasti insiden keselamatan aset ICT atau keadaan yang mengancam keselamatan aset ICT. Dengan itu, semua log yang berkaitan dengan aset ICT perlu disimpan bagi tujuan jejak audit.

6. Pematuhan

   PKS JPA hendaklah dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT.

7. Pemulihan

   Pemulihan sistem amat perlu untuk memastikan ketersediaan dan kebolehcapaian bagi meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui proses penduaan (backup) dan mewujudkan *Disaster Recovery Plan* (DRP) di bawah Pengurusan Kesinambungan Perkhidmatan (PKP).

8. Saling Bergantung

   Setiap prinsip adalah saling lengkap-melengkapi dan bergantung antara satu sama lain. Dengan itu tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan, dapat menjamin keselamatan yang maksimum.

PENILAIAN RISIKO KESELAMATAN ICT

JPA hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat daripada ancaman dan kerentanan (*vulnerability*) yang semakin meningkat hari ini. Justeru itu, JPA perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

JPA hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat JPA termasuklah aplikasi, perisian, peralatan, *server*, rangkaian, pangkalan data, sumber manusia, proses, dan prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem sokongan lain.

JPA bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 3 Tahun 2024: Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam.

JPA perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

1. Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
2. Menerima atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan atasan;
3. Mengelak atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak atau mencegah berlakunya risiko; dan
4. Memindahkan risiko kepada Pihak Luaran yang berkepentingan.

BAB 1

KAWALAN ORGANISASI

1.1 Polisi untuk Keselamatan Maklumat

Objektif

Memastikan polisi keselamatan maklumat bersesuaian, berterusan dan seiring dengan hala tuju pengurusan dalam menyokong keselamatan maklumat selari dengan fungsi JPA, undang-undang dan keperluan kontrak perjanjian.

1.1.1 Pelaksanaan Polisi	Tanggungjawab
Polisi Keselamatan Siber (PKS) JPA ini akan dikuat kuasakan oleh Ketua Pengarah Perkhidmatan Awam (KPPA), dan dibantu oleh Jawatankuasa Pemandu ICT JPA (JPICT) yang terdiri daripada Ketua Pegawai Digital (CDO), Pegawai Keselamatan ICT (ICTSO) dan semua Pengarah Bahagian.	Ketua Pengarah Perkhidmatan Awam (KPPA) penurunan kuasa kepada TKPPA(O)

1.1.2 Penyebaran Polisi	Tanggungjawab
Polisi ini hendaklah dipaparkan kepada umum dan disebarkan kepada semua Warga JPA dan Pihak Ketiga. Sebarang perubahan yang telah dipersetujui oleh JPICT, hendaklah dimaklumkan kepada semua pengguna JPA.	ICTSO

1.1.3 Penyelenggaraan Polisi	Tanggungjawab
PKS JPA adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan PKS JPA: a) mengenal pasti dan menentukan perubahan yang diperlukan; b) mengemukakan cadangan untuk pertimbangan Mesyuarat Jawatankuasa Keselamatan ICT (JKICT); c) memaklumkan cadangan pindaan untuk perakuan oleh JKICT dan kelulusan JPICT; d) memaklumkan pindaan yang telah diluluskan oleh JPICT kepada semua pengguna; dan e) menyemak semula dokumen sekurang-kurangnya setahun sekali atau mengikut keperluan bagi memastikan dokumen sentiasa relevan.	ICTSO JKICT

1.1.4 Pematuhan Polisi	Tanggungjawab
PKS JPA mestilah dipatuhi oleh semua pengguna	Pengguna

1.2 Peranan dan Tanggungjawab Keselamatan Maklumat

Objektif

Mewujudkan struktur, peranan dan tanggungjawab dalam pengurusan keselamatan maklumat di JPA.

1.2.1 Ketua Pengarah Perkhidmatan Awam (KPPA)	Tanggungjawab
Peranan dan tanggungjawab KPPA adalah seperti yang berikut: a) memastikan semua keperluan jabatan seperti sumber kewangan, sumber kakitangan dan perlindungan keselamatan adalah mencukupi; dan b) mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT (JPICT)	Ketua Pengarah Perkhidmatan Awam (KPPA)

1.2.2 Ketua Pegawai Maklumat (CDO)	Tanggungjawab
Jawatan Ketua Pegawai Digital (CDO) adalah disandang oleh Timbalan Ketua Pengarah Perkhidmatan Awam (Operasi). Peranan dan tanggungjawab CDO adalah seperti yang berikut: a) bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT JPA; b) bertanggungjawab menyelaras dan mengurus pelan tindakan dan program keselamatan seperti penyediaan PKS JPA, pelan latihan dan kesedaran pengguna, pengurusan risiko dan pengauditan; dan c) menentukan keperluan keselamatan ICT.	CDO

1.2.3 Pegawai Keselamatan ICT (ICTSO)	Tanggungjawab
Jawatan Pegawai Keselamatan ICT (ICTSO) adalah disandang oleh Pengarah Bahagian Digital dan Teknologi Maklumat (BDTM) JPA. Peranan dan tanggungjawab ICTSO adalah seperti yang berikut: a) mempengerusikan Mesyuarat Jawatankuasa Keselamatan ICT (JKICT); b) memastikan pengurusan risiko dan audit keselamatan ICT berpandukan kepada peraturan semasa yang sedang berkuat kuasa; c) memastikan langkah-langkah pengukuhan keselamatan dilaksanakan bagi meminimumkan ancaman keselamatan maklumat; d) melaporkan insiden keselamatan ICT kepada pihak *National Cyber Security Agency* (NACSA) dan seterusnya membantu dalam penyiasatan atau pemulihan; e) mewujudkan program-program bagi meningkatkan pengetahuan, kesedaran dan pembudayaan mengenai teknologi dan mekanisme kawalan maklumat dan aset ICT, ancaman-ancaman siber serta peranan dan tanggungjawab pengguna dalam mengendalikan kemudahan ICT di JPA; f) menyebar dan menyalurkan amaran awal terhadap ancaman-ancaman yang berpotensi menyebabkan kerosakan besar kepada aset ICT JPA; g) memastikan pengurusan bencana dan pengendalian insiden dilaksanakan mengikut peraturan semasa yang berkuat kuasa; h) memastikan pematuhan PKS JPA oleh pihak berkepentingan yang mengurus, mengguna dan mencapai aset serta perkhidmatan ICT Jabatan; i) menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan ICT; j) memastikan PKS JPA sentiasa relevan dengan arahan jabatan, peraturan semasa, perubahan teknologi, serta ancaman dalaman dan luaran; dan k) memastikan Pelan Strategik Pendigitalan (PSP) JPA mengandungi aspek keselamatan ICT.	ICTSO

1.2.4 Pengurus ICT

Tanggungjawab

Pengurus ICT

Jawatan Pengurus ICT disandang oleh dua (2) orang pegawai iaitu Pengarah Bahagian Digital dan Teknologi Maklumat dan Ketua Pusat Pengajian Teknologi Maklumat dan Pembangunan Teknologi (IMATEC), INTAN.

Peranan dan tanggungjawab Pengurus ICT adalah seperti yang berikut:

a) memastikan PKS JPA dilaksanakan dan dipatuhi di bahagian;
b) memastikan semua pengguna di JPA mematuhi dasar, piawaian dan garis panduan keselamatan ICT, dan seterusnya melaporkan sebarang insiden berkaitan keselamatan ICT;
c) mengkaji semula aspek-aspek keselamatan fizikal seperti kemudahan *backup* dan persekitaran pejabat yang perlu, dengan persetujuan ICTSO;
d) melaksanakan keperluan PKS dalam operasi semasa seperti yang berikut:
    i. pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu;
    ii. pembelian atau peningkatan perisian dan sistem komputer;
    iii. perolehan teknologi dan perkhidmatan komunikasi baharu;
    iv. pelantikan pembekal, perunding atau rakan usaha sama; dan
    v. menentukan pembekal, perunding atau rakan usaha sama menjalani tapisan keselamatan selaras dengan keperluan tahap perkhidmatan.
e) memastikan bentuk ancaman keselamatan terkini dikenal pasti dan penemuan ancaman dilaporkan kepada ICTSO;
f) menyemak dan mengesahkan garis panduan, prosedur dan tatacara bagi semua aplikasi yang dibangunkan di bahagian-bahagian agar mematuhi keperluan PKS JPA;
g) membangun, mengkaji semula dan mengemas kini pelan kontingensi dengan mengaktifkan *Disaster Recovery Plan* (*DRP*);
h) memastikan sistem kawalan capaian pengguna ke atas aset-aset ICT JPA dilaksanakan; dan
i) memastikan aspek keselamatan maklumat dilaksanakan dalam setiap pengurusan projek.

1.3 Pengasingan Tugas

Objektif

Menerangkan perbezaan tugas setiap individu dengan lebih jelas dan teratur untuk mencegah daripada berlakunya kebocoran serta kesilapan.

1.3.1 Pentadbir ICT JPA	Tanggungjawab
Pentadbir ICT JPA terdiri daripada seperti yang berikut: a) Pentadbir Rangkaian dan Keselamatan; b) Pentadbir Pangkalan Data; c) Pentadbir Portal; d) Pentadbir Pusat Data; e) Pentadbir Sistem Aplikasi; f) Pentadbir E-mel; g) Pentadbir Media Sosial JPA; dan h) Pegawai Aset ICT.	Pentadbir ICT JPA

1.3.1.1 Pentadbir Rangkaian dan Keselamatan	Tanggungjawab
Peranan dan tanggungjawab Pentadbir Rangkaian dan Keselamatan adalah seperti yang berikut: a) memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di JPA beroperasi sepanjang masa; b) memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna; c) merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; d) mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil; e) melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT; f) memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian JPA secara tidak sah; g) menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian; h) memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian; dan i) memastikan maklumat perhubungan perlu dikemas kini dari semasa ke semasa.	Pentadbir Rangkaian dan Keselamatan

1.3.1.2 Pentadbir Pangkalan Data	Tanggungjawab
Peranan dan tanggungjawab Pentadbir Pangkalan Data adalah seperti yang berikut: a) melaksanakan instalasi dan penambahbaikan pangkalan data serta perisian lain yang berkaitan dengan pangkalan data; b) memastikan pangkalan data boleh digunakan pada setiap masa; c) melaksanakan pemantauan dan penyelenggaraan yang berterusan ke atas pangkalan data; d) melaksanakan *data masking* dalam menyediakan data latihan; e) memastikan aktiviti pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur; f) melaksanakan polisi pengguna pangkalan data berdasarkan kepada prinsip- prinsip PKS; g) melaksanakan proses perkemasan data (*housekeeping*) di dalam pangkalan data; h) memantau proses *backup* dan *restoration* ke atas pangkalan data; dan i) melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO.	Pentadbir Pangkalan Data

1.3.1.3 Pentadbir Portal	Tanggungjawab
Peranan dan tanggungjawab Pentadbir Portal adalah seperti yang berikut: a) menerima kandungan portal yang telah disahkan kesahihan dan terkini daripada sumber yang sah; b) memantau prestasi capaian dan menjalankan penalaan prestasi untuk memastikan akses yang lancar; c) memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubah suai antara muka portal; d) mengasingkan kandungan dan aplikasi dalam talian untuk capaian secara Intranet dan Internet ke portal JPA; e) memastikan hanya maklumat yang bersifat terbuka dipaparkan di portal; f) memastikan reka bentuk portal dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; g) melaksanakan pengukuhan keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di *web server*; h) memantau proses *backup* dan *restoration* ke atas kandungan dan aplikasi portal; dan	Pentadbir Portal

i) melaporkan sebarang pelanggaran keselamatan portal kepada ICTSO.

1.3.1.4 Pentadbir Pusat Data	Tanggungjawab
Peranan dan tanggungjawab Pentadbir Pusat Data adalah seperti yang berikut: a) memastikan persekitaran fizikal dan keselamatan pusat data berada dalam keadaan baik dan selamat; b) memastikan keselamatan data dan sistem aplikasi yang berada dalam pusat data; c) menjadualkan dan melaksanakan proses *backup* dan *restoration* ke atas pangkalan data dan sistem secara berkala; d) menyediakan perancangan Pelan Pemulihan Bencana (PPB); e) memastikan pusat data sentiasa beroperasi mengikut polisi yang telah ditetapkan; f) melaporkan sebarang pelanggaran keselamatan Pusat Data JPA kepada ICTSO; dan g) memastikan maklumat perhubungan perlu dikemas kini dari semasa ke semasa.	Pentadbir Pusat Data

1.3.1.5 Pentadbir Sistem Aplikasi	Tanggungjawab
Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti yang berikut: a) mengkaji cadangan pembangunan, pembaikan, penyelarasan, penambahbaikan, pelaksanaan, pemantauan dan penyelenggaraan sistem di JPA; b) menyediakan dokumentasi sistem dan manual pengguna; c) memastikan *virus pattern, hotfix* dan *patch* yang berkaitan dengan sistem aplikasi dikemas kini supaya terhindar daripada ancaman virus dan penggodam; d) mengehadkan capaian ke atas dokumentasi sistem bagi mengelakkan dari penyalahgunaannya; e) memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas; f) memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaannya; g) mematuhi dan melaksanakan prinsip-prinsip PKS dalam pewujudan akaun pengguna ke atas setiap sistem aplikasi; dan h) melaporkan kepada ICTSO jika berlakunya insiden keselamatan ke atas sistem aplikasi.	Pentadbir Sistem Aplikasi

1.3.1.6 Pentadbir E-mel	Tanggungjawab
Peranan dan tanggungjawab Pentadbir E-mel adalah seperti yang berikut: a) menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan. Pembatalan akaun (pengguna yang tamat perkhidmatan, bertukar dan melanggar dasar dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat; b) pentadbir e-mel boleh membekukan akaun pengguna berdasarkan peraturan atau polisi semasa; c) memastikan pengguna e-mel JPA berkemahiran menggunakan e-mel melalui penyediaan dokumen tatacara penggunaan e-mel JPA dan Internet JPA serta pelaksanaan Kursus Pembudayaan ICT (Penggunaan E-mel dan Internet) secara berterusan; d) memastikan kemudahan mengakses capaian e-mel melalui pelbagai peralatan ICT dan alat komunikasi; e) melaporkan kepada ICTSO jika berlakunya insiden keselamatan ke atas sistem e-mel; dan f) memastikan maklumat perhubungan perlu dikemas kini dari semasa ke semasa.	Pentadbir E-mel

1.3.1.7 Pentadbir Media Sosial JPA	Tanggungjawab
Peranan dan tanggungjawab Pentadbir Media Sosial JPA adalah seperti yang berikut: a) mematuhi segala peraturan atau syarat-syarat yang digariskan oleh penyedia platform media sosial; b) mentadbir dan menyemak ketepatan serta sensitiviti maklumat dalam pengurusan kandungan (video, audio, gambar dan dokumen) dan komen mengikut etika media sosial semasa; dan c) melaporkan sebarang pelanggaran polisi atau etika penggunaan media sosial yang sedang berkuat kuasa kepada Ketua Komunikasi Korporat, JPA.	Pentadbir Media Sosial

1.3.1.8 Pegawai Aset ICT	Tanggungjawab
Pegawai Aset ICT ialah pegawai yang dilantik oleh Pegawai Pengawal. Peranan dan tanggungjawab Pegawai Aset ICT adalah seperti yang berikut: a) memastikan pengurusan aset ICT Kerajaan dijalankan selaras dengan peraturan yang ditetapkan; b) memastikan penerimaan aset ICT Kerajaan dilaksanakan oleh pegawai yang dilantik oleh Ketua Jabatan/ Bahagian; c) memastikan semua aset ICT Kerajaan yang diterima, didaftarkan menggunakan Sistem Pemantauan Pengurusan Aset (SPPA) dalam tempoh dua (2) minggu dari tarikh pengesahan penerimaan aset; d) memastikan semua aset ICT Kerajaan yang dipinjam, direkodkan ke dalam Rekod Pergerakan Aset. Aset tidak dibenarkan dibawa keluar dari pejabat kecuali dengan kelulusan secara bertulis daripada Ketua Jabatan/ Pegawai Aset/ Pegawai-pegawai lain yang diberi kuasa oleh Ketua Jabatan; e) memastikan Daftar Aset ICT dikemas kini apabila berlaku penambahan/ penggantian/ naik taraf aset termasuk selepas pemeriksaan aset, pelupusan dan hapus kira; f) memastikan semua aset ICT Kerajaan diberi tanda pengenalan dengan cara melabel tanda Hak Kerajaan Malaysia dan nama JPA/ Bahagian/ Agensi berkenaan di tempat yang mudah dilihat dan sesuai pada aset berkenaan; g) memastikan semua aset ICT Kerajaan ditandakan dengan Nombor Siri Pendaftaran mengikut susunan yang ditetapkan; h) memastikan senarai daftar induk aset ICT Kerajaan disediakan; i) memastikan senarai aset ICT Kerajaan disediakan mengikut lokasi dan format Senarai Aset ICT Kerajaan dalam dua (2) buah salinan. Satu (1) senarai berkenaan perlu disimpan oleh Pegawai Aset ICT/ Pembantu Pegawai Aset ICT dan satu (1) salinan perlu dipaparkan oleh pegawai yang bertanggungjawab di lokasi; j) memastikan setiap kerosakan aset ICT Kerajaan dilaporkan untuk tujuan penyelenggaraan; k) bertanggungjawab untuk menyedia, merancang, melaksana, memantau dan merekodkan penyelenggaraan aset ICT Kerajaan; l) merancang, memantau dan memastikan pemeriksaan aset ICT Kerajaan dilaksanakan ke atas keseluruhan aset ICT Kerajaan sekurang-kurangnya sekali setahun; dan m) memastikan setiap kes kehilangan aset ICT Kerajaan dilaporkan dan diuruskan dengan teratur.	Pegawai Aset ICT

1.4 Tanggungjawab Pengurusan

Objektif

Memastikan pihak pengurusan dan Warga JPA memahami peranan serta memenuhi tanggungjawab dalam keselamatan maklumat.

1.4.1 Tanggungjawab Pengurusan	Tanggungjawab
Perkara yang perlu dipastikan adalah seperti berikut:	CDO
a) memastikan semua Warga JPA dan pihak ketiga diberi taklimat berkaitan pematuhan ke atas PKS JPA; b) memastikan Warga JPA dan pihak ketiga bertanggungjawab ke atas keselamatan Aset ICT berdasarkan peraturan yang ditetapkan oleh JPA; dan **c)** memastikan sumber yang mencukupi untuk melaksanakan proses dan kawalan yang berkaitan keselamatan JPA.	ICTSO

1.4.1.1 Jawatankuasa Pemandu ICT (JPICT) JPA	Tanggungjawab
Keanggotaan JPICT adalah seperti yang berikut:	KPPA
Pengerusi: KPPA / TKPPA(O) (sekiranya diturunkan kuasa)	CDO
Ahli: a) Pengarah Bahagian Perkhidmatan; b) Pengarah Bahagian Perjawatan dan Organisasi; c) Pengarah INTAN; d) Pengarah Bahagian Pembangunan Modal Insan; e) Pengarah Bahagian Khidmat Pengurusan; f) Pengarah Bahagian Gaji dan Elaun; g) Pengarah Bahagian Pencen; h) Pengarah Bahagian Penyelidikan, Perancangan dan Dasar; i) Pengarah Bahagian Pengurusan Psikologi; j) Pengarah Bahagian Digital dan Teknologi Maklumat; k) Timbalan-Timbalan Pengarah Bahagian Digital dan Teknologi Maklumat;	

l) Ketua Pusat Pengajian Teknologi Maklumat dan Pembangunan Teknologi (IMATEC), INTAN;
m) Ketua Unit Komunikasi Korporat;
n) Penasihat Undang-undang (PUU);
o) Ketua Unit Audit Dalam; dan
p) Ketua Unit Integriti.

Urus setia: BDTM

Bidang kuasa:

a) menetapkan arah tuju dan strategi ICT untuk pelaksanaan ICT JPA;
b) merancang, menyelaras dan memantau pelaksanaan program atau projek ICT JPA;
c) menyelaras dan menyeragamkan pelaksanaan ICT agar selari dengan Pelan Strategik Pendigitalan (PSP) JPA dan PSP Sektor Awam;
d) meluluskan projek-projek ICT;
e) mengikuti dan memantau perkembangan program ICT serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT;
f) merancang dan menentukan langkah-langkah keselamatan ICT;
g) mengemukakan laporan kemajuan projek ICT yang diluluskan kepada JTICT/JPICT;
h) menetapkan dasar dan prosedur pengurusan portal JPA; dan
i) meluluskan dokumen PKS JPA.

1.4.1.2 Jawatankuasa Keselamatan ICT (JKICT) JPA	Tanggungjawab
Keanggotaan JKICT adalah seperti yang berikut:	ICTSO

Pengerusi: ICTSO

Ahli:

a) Ketua CSIRTJPA;

b) Pentadbir Pusat Data BDTM dan INTAN;

c) Pentadbir Sistem (*System Administrator*) BDTM dan INTAN;

d) Pentadbir Sistem Aplikasi BDTM dan INTAN;

e) Pentadbir Rangkaian dan Keselamatan (*Network and Security Administrator*) BDTM dan INTAN;

f) Pentadbir Portal (*Webmaster*) BDTM dan INTAN;

g) Pentadbir Pangkalan Data (*Database Administrator*) BDTM dan INTAN;

h) Penyelaras ICT Bahagian;

i) Pegawai Meja Bantuan (*Helpdesk Officer*) BDTM dan INTAN;

j) Perunding Latihan INTAN;

k) Wakil Pegawai Keselamatan JPA dan INTAN;

l) Wakil Pasukan Pelaksana ISMS BDTM; dan

m) Wakil Pasukan Pelaksana ISMS INTAN.

Urus setia: BDTM

Bidang kuasa:

a) menyelenggara dan memperakukan dokumen PKS JPA;
b) memantau tahap pematuhan PKS JPA;
c) menilai aspek teknikal keselamatan projek-projek ICT;
d) membangunkan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam jabatan yang mematuhi keperluan PKS JPA;
e) menyemak semula sistem ICT supaya sentiasa mematuhi keperluan keselamatan dari semasa ke semasa;
f) menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT;
g) memastikan PKS JPA selaras dengan dasar-dasar ICT kerajaan semasa;

h) bekerjasama dengan CSIRTJPA untuk mendapatkan maklum balas dan insiden untuk tindakan penyelenggaraan PKS JPA;
i) membincang tindakan yang melibatkan pelanggaran PKS JPA;
j) merancang dan menyelaras pensijilan ISMS seperti:
   i. struktur organisasi ISMS;
   ii. kursus kesedaran ISMS;
   iii. skop ISMS;
   iv. melaksanakan analisis jurang;
   v. merancang takwim aktiviti ISMS;
   vi. membantu Pelaksana ISMS menyediakan pernyataan dasar ISMS, *Statement of Applicability* (SoA), penilaian risiko, *risk treatment plan*, kaedah pengukuran kawalan dan prosedur-prosedur ISMS; dan
   vii. permohonan pensijilan.
k) mengemukakan isu dan masalah ISMS, jika ada; dan
l) membantu mengukur keberkesanan kawalan dan pelaksanaan ISMS.

1.4.1.3 *Cyber Security Incident Response Team* (CSIRT) JPA	Tanggungjawab
Keanggotaan CSIRTJPA adalah seperti yang berikut:	TP(M)T, BDTM

Pengerusi: TP(M)T, BDTM

Ahli:

a) Pegawai Teknologi Maklumat BDTM dan INTAN; dan
b) Penolong Pegawai Teknologi Maklumat BDTM dan INTAN.

Urus setia: BDTM

Bidang kuasa:

a) menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden;
b) merekod dan menjalankan siasatan awal insiden yang diterima;
c) menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum;
d) menghubungi dan melaporkan insiden yang berlaku kepada ICTSO dan pihak NACSA sama ada sebagai input atau untuk tindakan seterusnya;
e) merujuk agensi-agensi di bawah kawalannya untuk mengambil tindakan pemulihan dan pengukuhan; dan

f) melaporkan sebarang maklum balas dan insiden keselamatan ICT kepada JKICT.

1.4.1.4 Pasukan Pemulihan Bencana (PPB) JPA	Tanggungjawab
Keanggotaan PPB JPA adalah seperti yang berikut:	TP(M)T, BDTM
Pengerusi: TP(M)T, BDTM	Ketua Seksyen Perkhidmatan ICT, IMATEC
Ahli: a) Pasukan Sistem dan Operasi Pusat Data; b) Pasukan Rangkaian dan Keselamatan; c) Pasukan Aplikasi; d) Pasukan Pangkalan Data; dan e) Pasukan Meja Bantuan.	
Urus setia: BDTM	
Bidang kuasa: a) membangunkan Dokumen *Distaster Recovery Plan* (DRP); b) menyediakan kemudahan pemulihan bencana atau *Disaster Recovery Centre* (DRC); c) menjalankan penilaian ke atas masalah dan jangkaan akibat bencana; d) memaklumkan pengurusan atasan berkenaan bencana, kemajuan pemulihan bencana dan masalah; e) mengaktifkan prosedur pemulihan bencana; f) mengkoordinasi operasi pemulihan; g) memantau operasi pemulihan dan memastikan jadual pemulihan dipatuhi; h) mendokumentasikan operasi pemulihan; dan i) mengkoordinasi simulasi pemulihan bencana.	

1.5 Hubungan dengan Pihak Berkuasa

Objektif

Menyediakan senarai perhubungan pihak berkuasa berkaitan sekiranya berlaku kejadian yang menjejaskan keselamatan maklumat dan perkhidmatan ICT.

Tanggungjawab Pengurusan	Tanggungjawab
Perkara yang perlu diambil kira berkaitan hubungan dengan pihak berkuasa adalah tidak terhad seperti berikut: a) Malaysian Emergency Response System 999 (Polis, Bomba, Agensi Pertahanan Awam Malaysia); b) National Disaster Management Agency (NADMA); c) National Cyber Security Agency (NACSA); d) CyberSecurity Malaysia.	ICTSO

1.6 Hubungan dengan Pihak Berkepentingan

Objektif

Memastikan maklumat yang diperlukan oleh pihak berkepentingan dengan JPA disediakan.

Tanggungjawab Pihak Berkepentingan	Tanggungjawab
Pihak berkepentingan terdiri daripada pembekal, perunding, pemegang taruh, pelawat dan pihak-pihak lain yang terlibat dalam pengurusan, penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan. Perkara yang perlu dipatuhi: a) mengenal pasti risiko ke atas keselamatan maklumat dan memastikan pelaksanaan kawalan yang sesuai ke atas maklumat tersebut; b) memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga; c) akses kepada aset ICT JPA perlu berlandaskan perjanjian dan peraturan yang telah ditetapkan. Perjanjian yang dimeterai perlu mematuhi perkara-perkara berikut: i. Akta Keselamatan Siber 2024 (Akta 854); ii. Perakuan Akta Rahsia Rasmi 1972; iii. Hak Harta Intelek; iv. Arahan Teknologi Maklumat 2007(*IT Instructions*); v. Tapisan Keselamatan; dan vi. PKS JPA.	ICTSO Pengurus ICT Pentadbir Sistem

d) melaksanakan keselamatan dan menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber JPA seperti di **LAMPIRAN 1,** serta Perakuan Akta Rahsia Rasmi 1972 bagi perakuan untuk tidak membocorkan sebarang maklumat rasmi yang diperoleh sepanjang berkhidmat dengan JPA seperti di **LAMPIRAN 2**; dan
e) pihak berkepentingan kategori pelawat sahaja dikecualikan daripada mematuhi peraturan a hingga d seperti di atas.

1.7 Risikan Ancaman

Objektif

Memastikan kawalan ancaman keselamatan terhadap JPA difahami, dianalisis dan kaedah tindakan yang bersesuaian.

Pengurusan Risikan Ancaman	Tanggungjawab
Operasi rangkaian dan infrastruktur JPA dipantau menggunakan perkakasan dan perisian tertentu. Rekod aktiviti dan log dikumpulkan dan dianalisis bagi mengenal pasti ancaman serangan siber bagi membolehkan tindakan mitigasi diambil secara tepat dan berkesan. Analisis yang dikenal pasti dikategorikan kepada tiga jenis maklumat ancaman iaitu kaedah serangan, metodologi serangan dan perincian maklumat penyerang.	ICTSO Pengurus ICT

1.8 Keselamatan Maklumat Dalam Pengurusan Projek

Objektif

Memastikan keselamatan maklumat diambil kira dalam pengurusan projek.

Keselamatan Maklumat Dalam Pengurusan Projek	Tanggungjawab
Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: i. objektif keselamatan maklumat hendaklah diambil kira dan dilaksanakan dalam pengurusan projek merangkumi semua fasa pelaksanaan projek; ii. pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan; dan	ICTSO Pengurus ICT Pentadbir Rangkaian dan Keselamatan Pentadbir Sistem Aplikasi Pentadbir Pusat Data

iii. penyediaan spesifikasi perolehan hendaklah memasukkan keperluan ciri-ciri keselamatan.	Pentadbir Portal Pentadbir Pangkalan Data

1.9 Maklumat Inventori dan Aset

Objektif

Memastikan pengurusan maklumat dan aset dikenal pasti, dikelaskan, direkodkan, diselenggarakan dan penempatan ditetapkan untuk perlindungan keselamatan.

1.9.1 Inventori dan Penempatan Maklumat Serta Aset ICT	Tanggungjawab
Semua maklumat dan Aset ICT di JPA hendaklah diuruskan mengikut peraturan dan tatacara yang berkuat kuasa seperti berikut: a) memastikan maklumat dan Aset ICT yang dikenal pasti direkodkan serta dikemas kini mengikut peraturan semasa yang berkuat kuasa. b) memastikan pengemaskinian maklumat berkaitan instalasi dan perubahan aset; c) maklumat pemilik Aset ICT, lokasi dan status Aset ICT hendaklah dikemas kini dari semasa ke semasa; d) setiap maklumat dan Aset ICT perlu diklasifikasikan mengikut kategori kerahsiaan; e) memastikan Aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja. Penukaran pemilik hendaklah dilaksanakan sekiranya terdapat perubahan; dan f) pemeriksaan Aset ICT hendaklah dilaksanakan sekurang-kurangnya satu kali setahun.	Pegawai Aset Pembantu Pegawai Aset Kerani Aset

1.9.2 Tanggungjawab Pemilik	Tanggungjawab
Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT JPA. Tanggungjawab yang perlu dipatuhi untuk memastikan semua aset ICT dikawal dan dilindungi: a) memastikan semua aset ICT dikenal pasti, dikelas, didokumen, diselenggara dan dilupus. Maklumat aset ICT direkod dan dikemas kini dalam Sistem Pemantauan Pengurusan Aset (SPPA) mengikut peraturan semasa yang sedang berkuat kuasa;	Pegawai Aset ICT Warga JPA

b) memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;
c) memastikan semua pemilik mengesahkan penempatan aset ICT yang ditempatkan di JPA;
d) memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan;
e) setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalan atau milikan;
f) penggunaan aset ICT JPA mestilah untuk tujuan tugas rasmi sahaja; dan
g) aset ICT yang perlu dibawa keluar atas urusan rasmi perlu mendapat kelulusan.

1.10 Penggunaan Maklumat dan Aset ICT yang Boleh Diterima Penggunaan Maklumat dan Aset yang Diterima

Objektif

Memastikan setiap maklumat dan Aset ICT yang berkaitan dilindungi, digunakan dan dikendalikan dengan sewajarnya.

1.10.1 Penggunaan Maklumat dan Aset ICT	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:	Warga JPA
a) warga JPA dan pihak ketiga yang mempunyai capaian ke atas maklumat dan Aset ICT hendaklah bertanggungjawab terhadap keperluan perlindungan serta pengendalian keselamatan maklumat;	Pihak Ketiga Pentadbir ICT JPA
b) menyediakan prosedur pengurusan pengendalian maklumat yang merangkumi penggunaan, kebenaran, perkongsian dan pemantauan maklumat; c) memastikan kawalan capaian yang dibenarkan mengikut tahap klasifikasi pengelasan maklumat; d) menyelenggarakan rekod berkaitan senarai pengguna yang dibenarkan untuk capaian maklumat; e) memastikan kawalan ke atas salinan maklumat, storan maklumat dan perlu melaksanakan pelabelan media storan dengan jelas; dan f) memperoleh kebenaran untuk melaksanakan pelupusan maklumat dan aset berdasarkan tatacara pelupusan semasa yang sedang berkuat kuasa.	Pengurus ICT

1.10.2 Pengendalian Maklumat dan Aset ICT	Tanggungjawab
Pengendalian Aset ICT hendaklah dilaksanakan mengikut Tatacara Pengurusan Aset Alih Kerajaan. Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut: a) aktiviti yang melibatkan pemprosesan maklumat seperti penyalinan, penyimpanan, penghantaran, perkongsian dan pemusnahan maklumat mestilah mengikut peraturan yang berkuat kuasa; b) menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; c) memeriksa maklumat dan menentukan maklumat tepat dan lengkap dari semasa ke semasa; d) menentukan maklumat sedia untuk digunakan; e) menjaga kerahsiaan kata laluan; dan f) mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;	Warga JPA

1.11 Pemulangan Aset ICT

Objektif

Memastikan proses pemulangan aset ICT dilaksanakan apabila berlaku perubahan dan penamatan perkhidmatan, kontrak atau perjanjian.

1.11.1 Pemulangan Aset ICT	Tanggungjawab
Memastikan semua Aset ICT dikembalikan kepada JPA mengikut peraturan dan terma perkhidmatan yang ditetapkan bagi pegawai yang: a) bertukar keluar; b) bersara; c) meninggal dunia; dan d) ditamatkan perkhidmatan; dan diarahkan oleh Ketua Jabatan.	Warga JPA Pegawai Aset Pembantu Pegawai Aset

1.11.2 Peminjaman Aset ICT	Tanggungjawab
Tatacara peminjaman aset adalah seperti yang berikut: a) mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh JPA bagi membawa keluar aset ICT bagi tujuan yang dibenarkan; b) melindungi dan mengawal aset ICT sepanjang masa; c) merekodkan aktiviti peminjaman dan pemulangan aset ICT; dan d) menyemak aset ICT ketika peminjaman dan pemulangan dilakukan.	Pentadbir Aset ICT Pemilik Aset Warga JPA

1.12 Klasifikasi Maklumat

Objektif

Memastikan pengenalpastian dan pemahaman tentang keperluan perlindungan maklumat mengikut kepentingan di JPA.

Pengelasan Maklumat	Tanggungjawab
Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan (Semakan dan Pindaan 2017) seperti yang berikut: a) Rahsia Besar; b) Rahsia; c) Sulit; d) Terhad; e) Dokumen Rasmi; dan f) Data Terbuka.	Pegawai Pengelas

1.13 Pelabelan Maklumat

Objektif

Memastikan pelabelan maklumat dilaksanakan bagi memudahkan pengurusan penyimpanan maklumat.

Pelabelan Maklumat	Tanggungjawab
Semua maklumat dilabelkan mengikut klasifikasi maklumat sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan (Semakan dan Pindaan 2017).	Pegawai Rekod Jabatan

1.14 Pemindahan Maklumat

Objektif

Memastikan keselamatan semasa pemindahan maklumat kepada pihak ketiga atau sebaliknya. Pemindahan maklumat secara dalaman atau luaran hendaklah mengikut syarat atau perjanjian yang ditetapkan.

1.14.1 Pemindahan Maklumat	Tanggungjawab
Penghantaran atau pemindahan maklumat yang mengandungi maklumat terperingkat boleh dilaksanakan melalui medium elektronik atau media storan fizikal. Penghantaran fail bersaiz besar boleh menggunakan kaedah muat turun fail dengan memaklumkan lokasi *Universal Resource Locator* (URL) atau kaedah pemampatan untuk mengurangkan saiz fail dengan memastikan ciri-ciri keselamatan dilaksanakan. a) kawalan ke atas pemindahan maklumat daripada dicerobohi, diubah, disalin, dimusnahkan dan sebagainya; b) pemindahan maklumat hendaklah direkodkan bagi kawalan pengesanan; c) menggunakan kaedah pengesahan yang selamat sekiranya pemindahan maklumat menggunakan rangkaian awam; d) memastikan maklumat elektronik yang hendak dipindahkan perlu dilindungi menggunakan enkripsi *Secure Socket Layer* (SSL) atau *Application Programming Interface* (API). e) pemindahan maklumat melalui media storan seperti *cloud storage, hard disk,* USB *flash drive* dan media storan lain perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan ketersediaan untuk digunakan; dan	ICTSO Pentadbir Rangkaian dan Keselamatan Pentadbir E-mel Warga JPA

f) penghantaran dokumen terperingkat mestilah menggunakan medium penghantaran rasmi jabatan.

1.15 Kawalan Capaian

Objektif

Memastikan akses bagi menghalang capaian yang tidak dibenarkan kepada maklumat dan lain-lain yang berkaitan aset.

1.15.1 Keperluan Kawalan Capaian	Tanggungjawab
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong kawalan capaian pengguna sedia ada.	ICTSO Pengurus ICT Pentadbir Sistem Aplikasi

1.15.2 Capaian Pengguna	Tanggungjawab
Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, Pentadbir Sistem perlu mengambil langkah-langkah berikut: a) akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan; b) akaun ID pengguna hendaklah mencerminkan identiti pengguna; c) pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika kaedah penggunaannya melanggar peraturan; d) penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan e) pemilik akaun dan capaian pengguna adalah tertakluk kepada peraturan jabatan dan tindakan pengemaskinian atau pembatalan hendaklah diambil atas sebab berikut: i. pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi sebulan; ii. bertukar bidang tugas kerja; iii. bertukar ke agensi lain; iv. bersara; atau ditamatkan perkhidmatan.	ICTSO Pengurus ICT Pentadbir Sistem Aplikasi

1.15.3 Hak Capaian	Tanggungjawab
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat, atas prinsip perlu mengetahui (need-to-know-basis). Keperluan capaian hendaklah sentiasa dipantau dan dikemas kini bagi memastikan hak capaian ini diberikan kepada pegawai dan kakitangan yang dibenarkan sahaja.	ICTSO Pengurus ICT Pentadbir Sistem Aplikasi

1.15.4 Capaian Sistem Pengoperasian	Tanggungjawab
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian terhadap sistem komputer. Kemudahan ini juga perlu bagi: a) mengenal pasti identiti/ terminal/ lokasi bagi setiap pengguna yang dibenarkan; b) merekodkan capaian yang berjaya dan gagal; c) membolehkan pengesahan kata laluan dilaksanakan berdasarkan kriteria kata laluan yang kukuh; dan d) mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user;*	ICTSO Pengurus ICT Pentadbir Sistem Aplikasi

1.15.5 Capaian Aplikasi dan Maklumat	Tanggungjawab
a) bertujuan melindungi sistem maklumat dan aplikasi sedia ada daripada sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. b) capaian sistem dan aplikasi di JPA adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut perlu dipatuhi: i. pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; ii. setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti- aktiviti yang tidak diingini; iii. menyediakan paparan dasar privasi/ notis penafian kepada pengguna ketika menggunakan aplikasi bagi melindungi maklumat daripada sebarang bentuk penyalahgunaan;	ICTSO Pengurus ICT Pentadbir Sistem Aplikasi

iv. memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan
v. maklumat tarikh *login* terakhir hendaklah direkodkan; digalakkan *session timeout* dilaksanakan.

1.15.6 Capaian Rangkaian	Tanggungjawab
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) mewujudkan segmen rangkaian yang bersesuaian bagi membezakan di antara rangkaian JPA dan rangkaian awam; b) mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dengan peralatan yang menepati kesesuaian penggunaannya; c) memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; d) capaian pengguna jarak jauh (remote user) perlulah dikawal dan dipantau; e) capaian fizikal dan logikal ke atas peralatan rangkaian bagi tujuan mengubah konfigurasi perlulah dikawal; dan f) semua rangkaian yang dikongsi (shared networks), terutama yang keluar daripada rangkaian JPA, polisi perlu diwujudkan untuk mengawal capai oleh pengguna.	ICTSO Pengurus ICT Pentadbir Rangkaian dan Keselamatan

1.15.7 Capaian Jarak Jauh	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) penghantaran maklumat yang menggunakan capaian jarak jauh mestilah menggunakan kaedah enkripsi (encryption); b) lokasi bagi akses ke sistem ICT JPA hendaklah dipastikan selamat; c) penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Pentadbir Rangkaian dan Keselamatan. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini; dan d) penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Pentadbir Rangkaian dan Keselamatan. Capaian jarak jauh hendaklah menggunakan kemudahan yang disediakan oleh jabatan.	ICTSO Pengurus ICT Pentadbir Rangkaian dan Keselamatan

1.15.8 Capaian Internet	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) penggunaan Internet di JPA hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian dan Keselamatan bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kawalan ini akan dapat melindungi daripada sebarang bentuk ancaman ke atas rangkaian JPA; b) penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; c) polisi *Content Filtering* mestilah digunakan dan dipantau bagi mengawal akses Internet. Pengguna boleh memohon pengecualian mengikut fungsi kerja untuk pertimbangan; dan d) penggunaan teknologi *packet shaper* adalah mengikut keperluan bagi menguruskan penggunaan *bandwidth* yang maksimum dan lebih berkesan.	ICTSO Pengurus ICT Pentadbir Rangkaian dan Keselamatan

1.16 Pengurusan Identiti

Objektif

Memastikan ID pengguna adalah unik dan sesuai ke atas entiti untuk mengakses sistem dan aset JPA lain yang berkaitan.

1.16.1 Proses Pengurusan Identiti	Tanggungjawab
Proses pengurusan identiti perlu memastikan perkara berikut dipatuhi: a) memastikan ID pengguna hendaklah unik dan pengguna bertanggungjawab ke atas akaun tersebut selepas pengesahan penerimaan dibuat; b) memastikan identiti yang diberikan kepada lebih dari seorang individu (identiti bersama) hanya dibenarkan jika ada keperluan dan tertakluk kepada kelulusan serta direkodkan; c) memastikan perkakasan yang memerlukan ID pengguna hendaklah mendapatkan kelulusan serta pengawasan berterusan; d) merekodkan semua penggunaan dan pengurusan identiti pengguna; e) pewujudan ID pengguna hendaklah mendapat sokongan oleh Ketua Bahagian/ Cawangan/ Unit/ PTB.	ICTSO Pengurus ICT Pentadbir Sistem Aplikasi Pihak Ketiga

f) membatalkan, menamatkan dan menukar peranan akaun pengguna berdasarkan pemakluman oleh Ketua Bahagian/ Cawangan /Unit/ PTB atas sebab berikut:
   i. bertukar bidang tugas kerja;
   ii. bertukar ke agensi lain;
   iii. bersara;
   iv. ditamatkan perkhidmatan; dan
   v. pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi tiga (3) bulan.
g) proses semakan akses pengguna perlu dilaksanakan untuk mengkaji semula kebenaran dan pembatalan capaian pengguna ke atas semua aplikasi dan perkhidmatan; dan
h) dilarang menggunakan nama atau menyamar sebagai individu lain dalam mana-mana perkhidmatan dalam talian.

1.16.2 Prosedur Penyediaan atau Pembatalan Akses	**Tanggungjawab**
Prosedur bagi penyediaan atau pembatalan akses perlu memastikan perkara berikut: a) memastikan identiti yang diwujudkan memenuhi keperluan tugasan berkaitan; b) mengesahkan identiti pengguna yang memohon sebelum pewujudan ID pengguna; c) mewujudkan ID pengguna; d) mengkonfigurasi dan mengaktifkan ID pengguna; dan e) menyediakan atau membatalkan hak akses berdasarkan kelulusan atau pemakluman.	Pengurus ICT Pentadbir Sistem Aplikasi

1.17 Pengesahan Maklumat

Objektif

Memastikan pengesahan entiti yang betul untuk mengelakkan kegagalan capaian maklumat.

1.17.1 Proses Pengesahan Maklumat	Tanggungjawab
Proses penyediaan dan pengurusan pengesahan maklumat perlu berdasarkan perkara berikut: a) penjanaan kata laluan peribadi sementara semasa proses pendaftaran yang unik untuk setiap individu. Pengguna diwajibkan menukar kata laluan apabila log masuk kali pertama; b) kata laluan *default* bagi Pihak Luaran perlu ditukar serta-merta selepas selesai pemasangan sistem, perkakasan atau perisian; dan c) menghantar kata laluan kepada pengguna dengan cara yang selamat.	ICTSO Pengurus ICT Pentadbir Sistem Aplikasi

1.17.2 Tanggungjawab Pengguna	Tanggungjawab
Setiap individu yang mempunyai akses hendaklah memastikan perkara berikut: a) merahsiakan kata laluan dan tidak dikongsi dengan sesiapa melainkan ID pengguna bersama yang diberi kebenaran sahaja; b) kata laluan yang telah terdedah kepada pihak tidak bertanggungjawab perlu ditukar serta-merta; c) kata laluan yang digunakan mestilah kukuh mengikut cadangan amalan terbaik seperti: i. kata laluan tidak boleh diteka atau diperoleh dengan mudah berdasarkan maklumat berkaitan individu (seperti nama, nombor telefon dan tarikh lahir); ii. kata laluan tidak berdasarkan perkataan kamus (dictionary words) atau gabungannya; iii. menggunakan kata laluan yang mudah diingat dan berkualiti iaitu sekurang-kurangnya minimum 12 gabungan aksara iaitu huruf besar, huruf kecil, simbol dan angka; dan iv. kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun.	Warga JPA Pihak Luaran

d) menggunakan pengurusan identiti secara berpusat yang selamat seperti *Active Directory* atau tidak menggunakan kata laluan yang sama untuk perkhidmatan dan sistem yang berlainan.

1.17.3 Sistem Pengurusan Kata Laluan **Tanggungjawab**

Sistem pengurusan kata laluan hendaklah mematuhi perkara berikut:

ICTSO

Pengurus ICT

Pentadbir Sistem Aplikasi

Warga JPA

a) membenarkan pengguna memilih dan menukar kata laluan mereka sendiri;
b) menguatkuasakan kata laluan yang kukuh mengikut cadangan amalan baik;
c) mewajibkan pengguna menukar kata laluan mereka pada pertama kali log masuk;
d) mewajibkan perubahan kata laluan sekiranya berlaku insiden keselamatan, penamatan atau kata laluan yang berkongsi identiti;
e) menghalang penggunaan kata laluan terdahulu dan mengelakkan penggunaan kata laluan yang berulang (5 kali sejarah);
f) menghalang penggunaan kata laluan yang mempunyai nama pengguna atau gabungan kata laluan daripada sistem yang pernah terdedah atau digodam;
g) tidak memaparkan kata laluan pada skrin apabila dimasukkan;
h) menyimpan dan menghantar kata laluan dalam bentuk yang dilindungi.
i) menukar kata laluan selepas 180 hari (6 bulan) melaksanakan penukaran kata laluan yang luput kepada yang baharu (rujuk Prosedur Pengurusan Kata Laluan); dan
j) penyulitan dan *hashing* hendaklah dilakukan terhadap kata laluan.

1.18 Hak Akses

Objektif

Memastikan hak akses kepada maklumat dan aset lain dibenarkan mengikut keperluan.

1.18.1 Pendaftaran dan Pembatalan Hak Akses	Tanggungjawab
Proses pendaftaran atau pembatalan hak akses fizikal dan logikal yang diberikan adalah seperti yang berikut: a) mendapatkan kebenaran daripada pemilik maklumat dan aset lain yang berkaitan untuk digunakan; b) mengambil kira polisi atau peraturan khas berkaitan hak akses; c) memastikan pengasingan peranan hak akses untuk mengelakkan percanggahan; d) memastikan hak akses dihentikan apabila pengguna tidak perlu mengakses maklumat; e) memberi hak akses sementara untuk kakitangan kontrak atau kakitangan yang memerlukan akses sementara; f) mengesahkan tahap akses yang diberikan adalah mengikut had capaian dan selari dengan keperluan keselamatan maklumat lain; g) memastikan bahawa hak akses diaktifkan selepas prosedur pengesahan diluluskan; h) menyelenggarakan rekod hak akses secara berpusat; i) melaksanakan perubahan hak akses pengguna yang telah bertukar peranan atau bertukar keluar; j) menamatkan atau mengemas kini hak akses fizikal atau logikal; dan k) menyelenggarakan rekod perubahan hak akses fizikal dan logikal pengguna.	ICTSO Pengurus ICT Pentadbir Sistem Aplikasi Pentadbir Rangkaian dan Keselamatan

1.18.2 Semakan Hak Akses	Tanggungjawab
Semakan berkala terhadap hak akses perlu dilaksanakan seperti perkara berikut: a) selepas berlaku perubahan dalam JPA seperti pertukaran kerja, kenaikan pangkat, penurunan pangkat atau penamatan; b) pengesahan hak akses *(*privileged access rights*)* c) selepas diluluskan; dan d) membuat semakan hak akses pengguna secara berkala atau sekurang-kurangnya satu kali setahun atau mengikut keperluan	Pentadbir Sistem Aplikasi Pentadbir Rangkaian dan Keselamatan

1.18.3 Pertimbangan Sebelum Pertukaran atau Penamatan Pekerjaan	Tanggungjawab
Hak akses pengguna kepada maklumat dan aset lain yang berkaitan perlu disemak, diselaraskan atau dinyahaktifkan sebelum sebarang perubahan atau penamatan berdasarkan penilaian faktor risiko seperti yang berikut: a) pengguna atau pengurusan mengemukakan sebarang permohonan penamatan dan perubahan; b) tanggungjawab semasa pengguna; dan c) nilai aset yang boleh dicapai.	Pengurus ICT Pentadbir Sistem Aplikasi Pentadbir Rangkaian dan Keselamatan

1.19 Keselamatan Maklumat dengan Pihak Luaran

Objektif

Memastikan semua Pihak Luaran adalah tertakluk kepada peraturan yang berkuat kuasa.

1.19.1 Keselamatan Maklumat ke Atas Pihak Luaran	Tanggungjawab
Keselamatan maklumat ke atas Pihak Luaran hendaklah mematuhi perkara seperti berikut: a) mengenal pasti dan merekodkan Pihak Luaran yang terlibat dengan aspek kerahsiaan, integriti dan ketersediaan maklumat JPA; b) mewujudkan kaedah penilaian dan pemilihan Pihak Luaran berdasarkan klasifikasi maklumat, produk dan perkhidmatan; c) menilai dan memilih produk atau perkhidmatan Pihak Luaran yang mempunyai kawalan keselamatan maklumat serta melaksanakan semakan berkala bagi memastikan integriti dan keselamatan maklumat terjamin; d) mengenal pasti maklumat JPA, perkhidmatan ICT dan infrastruktur fizikal yang boleh diakses, dipantau, dikawal atau digunakan oleh Pihak Luaran; e) mengenal pasti jenis komponen dan perkhidmatan infrastruktur ICT yang disediakan oleh Pihak Luaran yang boleh menjejaskan kerahsiaan, integriti dan ketersediaan maklumat JPA; f) menilai dan mengurus risiko keselamatan maklumat yang berkaitan dengan: i. penggunaan maklumat dan aset Pihak Luaran; ii. kerosakan (malfunction) atau kelemahan produk (termasuk komponen perisian dan subkomponen); atau iii. perkhidmatan yang disediakan oleh Pihak Luaran;	Pengurus ICT Pentadbir Sistem

g) memantau pematuhan dan keperluan keselamatan maklumat yang ditetapkan kepada semua Pihak Luaran;
h) mencegah ketidakpatuhan Pihak Luaran, sama ada dikesan melalui pemantauan atau sumber lain;
i) pengurusan insiden berkaitan produk atau perkhidmatan di bawah tanggungjawab JPA dan Pihak Luaran;
j) keupayaan tindakan pemulihan dan pelan kontingensi (contingency plan) untuk memastikan ketersediaan maklumat;
k) program kesedaran dan latihan kepada kakitangan JPA yang melibatkan dengan Pihak Luaran termasuk mempunyai akses kepada maklumat;
l) memastikan keselamatan maklumat sentiasa terjaga sepanjang tempoh pemindahan maklumat atau aset lain yang berkaitan;
m) memastikan keselamatan maklumat semasa penamatan perkhidmatan Pihak Luaran merangkumi perkara berikut:
    i. pembatalan hak akses;
    ii. pengendalian maklumat;
    iii. menentukan pemilikan harta intelek;
    iv. pemindahan maklumat sekiranya berlaku pertukaran Pihak Luaran;
    v. pengurusan rekod;
    vi. pemulangan aset;
    vii. pelupusan maklumat dan aset lain berkaitan secara selamat; dan
    viii. keperluan kerahsiaan yang berterusan.
n) tahap keselamatan kakitangan dan keselamatan fizikal yang perlu dipatuhi Pihak Luaran dengan mematuhi keperluan berikut:
    i. Polisi Keselamatan Siber (PKS) JPA;
    ii. Akta Rahsia Rasmi 1972; dan
o) tapisan keselamatan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO).

1.20 Keselamatan Maklumat Dalam Perjanjian Pihak Luaran

Objektif

Memastikan keselamatan maklumat dengan Pihak Luaran melalui perjanjian yang telah dipersetujui.

1.20.1 Kawalan Keselamatan Maklumat Melalui Perjanjian dengan Pihak Luaran	Tanggungjawab
Perjanjian dengan Pihak Luaran perlu diwujudkan untuk memastikan pemahaman yang jelas antara JPA dan Pihak Luaran mengenai tanggungjawab kedua-dua pihak. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) keterangan serta kaedah maklumat yang boleh diakses; b) pengelasan klasifikasi maklumat berdasarkan kategori rekod rasmi Kerajaan; c) keperluan undang-undang, peraturan dan kontrak, termasuk perlindungan data, pengendalian maklumat pengenalan peribadi, hak harta intelek dan hak cipta; d) kewajipan mematuhi kontrak perjanjian yang dipersetujui termasuk mematuhi keperluan keselamatan yang telah ditetapkan oleh JPA; e) peraturan penggunaan maklumat dan aset lain yang berkaitan; f) prosedur atau syarat kebenaran penggunaan, penamatan dan penggunaan maklumat JPA serta aset lain yang berkaitan dengan kakitangan Pihak Luaran; g) keperluan keselamatan maklumat bagi infrastruktur ICT Pihak Luaran yang mempunyai akses ke atas maklumat JPA; h) ganti rugi dan langkah pemulihan bagi kegagalan pematuhan kontrak oleh Pihak Luaran; i) keperluan dan prosedur pengurusan insiden keselamatan; j) keperluan latihan dan program kesedaran untuk topik khusus keselamatan maklumat; k) klausa yang berkaitan penglibatan subkontrak termasuk kawalan perlu dimasukkan dalam perjanjian; l) maklumat pegawai perhubungan bagi pelaporan isu keselamatan maklumat; m) pelaksanaan tapisan keselamatan kakitangan Pihak Luaran mengikut undang-undang yang berkuat kuasa; n) laporan jaminan pengesahan keselamatan maklumat dan pembuktian oleh Pihak Luaran; o) hak untuk mengaudit Pihak Luaran bagi proses dan kawalan yang terkandung dalam kontrak perjanjian;	Pengurus ICT Pihak Luaran

p) obligasi Pihak Luaran menyediakan laporan secara berkala berkaitan keberkesanan kawalan dan tindakan pembetulan terhadap isu berbangkit dalam masa yang ditetapkan;
q) penyelesaian ketidakpatuhan dan proses penyelesaian konflik;
r) menyediakan sandaran (backup) berdasarkan keperluan JPA dari segi kekerapan, jenis dan lokasi penyimpanan;
s) memastikan ketersediaan tapak alternatif pemulihan bencana sekiranya tapak utama gagal berfungsi;
t) menyediakan proses pengurusan perubahan;
u) kawalan keselamatan fizikal yang selari dengan tahap klasifikasi maklumat;
v) kawalan pemindahan terhadap maklumat fizikal atau logikal;
w) klausa penamatan selepas perjanjian merangkumi pengurusan rekod, pemulangan aset, pelupusan maklumat dan aset lain yang berkaitan secara selamat berdasarkan pematuhan kerahsiaan semasa;
x) maklumat yang disimpan oleh Pihak Luaran hendaklah dihapus dengan selamat jika tidak lagi diperlukan; dan
y) memastikan penyerahan dokumen dilaksanakan kepada JPA atau pihak lain sebelum kontrak tamat.

1.21 Pengurusan Keselamatan Maklumat Dalam Rantaian Maklumat dan Komunikasi ICT

Objektif

Memastikan persetujuan kawalan keselamatan bersama Pihak Luaran dimeterai.

1.21.1 Kawalan Rantaian Bekalan Maklumat dan Komunikasi	Tanggungjawab
Perjanjian dengan Pihak Luaran hendaklah mengambil kira keperluan keselamatan maklumat untuk menangani risiko yang berkaitan dengan rantaian bekalan maklumat dan komunikasi. Perkara yang perlu diambil kira adalah seperti yang berikut: a) menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; b) Pihak Luaran hendaklah menghebahkan keperluan keselamatan maklumat kepada subkontraktor bagi perkhidmatan; c) melaksanakan satu proses/ kaedah pemantauan yang boleh mengesahkan Pihak Luaran produk dan perkhidmatan mematuhi keperluan keselamatan maklumat JPA;	Pengurus ICT Pihak Luaran

d) memastikan jaminan daripada Pihak Luaran bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik;
e) memastikan komponen produk yang dibekalkan adalah tulen dan tidak diubah daripada spesifikasi asal atau mengikut keperluan JPA;
f) memastikan bahawa produk ICT memenuhi standard keselamatan yang ditetapkan atau melalui proses pensijilan rasmi atau amalan terbaik;
g) menentukan kaedah-kaedah bagi perkongsian maklumat mengenai rantaian bekalan (supply chain) antara JPA dan Pihak Luaran; dan
h) memastikan pengurusan kitaran hayat dan ketersediaan komponen ICT yang tidak lagi tersedia disebabkan Pihak Luaran tidak lagi beroperasi atau Pihak Luaran tidak lagi menyediakan komponen ini disebabkan kemajuan teknologi. Ini bagi mengurangkan impak risiko keselamatan ke atas JPA.

1.22 Pemantauan, Semakan dan Pengurusan Perubahan Perkhidmatan Pihak Luaran

Objektif

Memastikan pemantauan, penilaian dan pengurusan perubahan dilaksanakan ke atas Pihak Luaran.

1.22.1 Pemantauan dan Penilaian Perkhidmatan Pihak Luaran	Tanggungjawab
Pemantauan, kaji semula dan penilaian perkhidmatan Pihak Luaran adalah seperti yang berikut: a) memastikan tahap perjanjian perkhidmatan Pihak Luaran selaras dengan kontrak perjanjian; b) laporan perkhidmatan yang dihasilkan oleh Pihak Luaran hendaklah dipantau dan status kemajuan dikemukakan kepada JPA; c) memaklumkan mengenai insiden keselamatan kepada Pihak Luaran dan mengkaji maklumat seperti yang dikehendaki dalam perjanjian; d) mengambil tindakan terhadap sebarang insiden keselamatan maklumat yang dikenal pasti; e) menguruskan kelemahan keselamatan maklumat yang dikenal pasti; dan	Pemilik Projek Pentadbir Sistem Aplikasi

f) Pihak Luaran yang didapati tidak memenuhi keperluan kontrak perjanjian boleh dikenakan tindakan bersesuaian seperti penalti.

1.22.2 Pengurusan Perubahan Perkhidmatan Pihak Luaran	Tanggungjawab
Setiap perubahan perkhidmatan Pihak Luaran hendaklah dilaksanakan secara teratur dan mengikut *Standard Operating Procedure* (SOP) yang ditetapkan. Perkara yang perlu diambil kira adalah seperti yang berikut: a) memastikan perubahan dalam perkhidmatan Pihak Luaran dipersetujui bersama dan menguntungkan pihak kerajaan; b) memastikan perubahan dalam perjanjian dengan Pihak Luaran mengambil kira maklumat kritikal JPA, sistem serta proses yang terlibat dan kajian risiko; c) pemantauan dan persetujuan ke atas perubahan perkhidmatan Pihak Luaran yang merangkumi perkara berikut: i. peningkatan kepada perkhidmatan/ produk sedia ada termasuk rangkaian, perisian, versi dan alatan pembangunan; ii. pembangunan sebarang aplikasi dan sistem baharu; iii. pengubahsuaian atau kemas kini polisi dan prosedur Pihak Luaran; iv. kaedah kawalan baharu atau yang dikemas kini bagi menyelesaikan insiden keselamatan maklumat dan meningkatkan keselamatan maklumat; dan v. perubahan lokasi perkakasan dan/ atau perkhidmatan.	Pengurus ICT Pentadbir Sistem Aplikasi

1.23 Keselamatan Maklumat Bagi Perkhidmatan Pengkomputeran Awan

Objektif

Memastikan pengurusan keselamatan maklumat bagi pengkomputeran awan.

1.23.1 Keselamatan Maklumat untuk Perkhidmatan Pengkomputeran Awan	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) mengenal pasti klasifikasi maklumat atau data dalam penggunaan perkhidmatan pengkomputeran awan; b) mengenal pasti ciri-ciri asas dan model perkhidmatan pengkomputeran awan yang hendak digunakan;	ICTSO Pengurus ICT Pentadbir Pusat Data

c) menetapkan tugas dan tanggungjawab ke atas pengurusan perkhidmatan awan;
d) menentukan tanggungjawab kawalan keselamatan perkhidmatan awan di antara penyedia dan pengguna perkhidmatan awan;
e) memastikan kemampuan dan jaminan kawalan keselamatan maklumat yang dilaksanakan oleh penyedia perkhidmatan awan;
f) struktur tadbir urus hendaklah dikenal pasti berdasarkan peranan dan tanggungjawab untuk merancang, mengurus dan mengawal polisi serta fungsi yang berkaitan dengan keselamatan maklumat dalam pengurusan pengkomputeran awan;
g) pematuhan pengurusan maklumat rahsia rasmi dalam persekitaran ICT menjadi prasyarat (prerequisite) terhadap sebarang cadangan penggunaan perkhidmatan pengkomputeran awan;
h) memastikan pengurusan kontrak dan terma keselamatan dalam penggunaan perkhidmatan pengkomputeran awan;
i) memastikan perlindungan migrasi data ke pengkomputeran awan, perlindungan data semasa penghantaran dan perlindungan data dalam simpanan logikal atau fizikal oleh pihak penyedia perkhidmatan;
j) memantau, menyemak dan menilai keselamatan maklumat dalam perkhidmatan pengkomputeran awan;
k) memastikan pengurusan insiden oleh penyedia perkhidmatan pengkomputeran awan;
l) memastikan penyedia perkhidmatan mewujudkan atau mempunyai pelan Pengurusan Kesinambungan Perkhidmatan (PKP); dan
m) memastikan penamatan perkhidmatan pengkomputeran awan dilaksanakan mengikut peraturan berkuat kuasa.

1.23.2 Pengurusan Kontrak Perkhidmatan Awan	**Tanggungjawab**
Perjanjian dengan penyedia perkhidmatan awan perlu mengandungi perkara berikut: a) menyediakan cadangan penggunaan berdasarkan piawaian yang bersesuaian; b) menguruskan kawalan akses ke perkhidmatan pengkomputeran awan berdasarkan keperluan JPA; c) melaksanakan pemantauan ke atas perisian hasad serta cadangan perlindungan;	ICTSO Pengurus ICT Pentadbir Pusat Data

d) memproses dan menyimpan maklumat rahsia rasmi JPA yang diluluskan sahaja;
e) memberikan khidmat sokongan sekiranya berlaku insiden keselamatan maklumat;
f) memastikan keperluan keselamatan maklumat dipenuhi sekiranya perkhidmatan pengkomputeran awan dilaksanakan oleh Pihak Luaran;
g) membantu JPA mengumpul bukti digital sekiranya diperlukan oleh undang-undang;
h) menyediakan khidmat sokongan yang bersesuaian sekiranya perkhidmatan awan tidak disambung guna;
i) menyediakan sandaran ke atas maklumat dan tetapan konfigurasi perkhidmatan awan; dan
j) menyediakan dan mengembalikan maklumat seperti fail konfigurasi, kod sumber dan maklumat JPA sekiranya perkhidmatan pengkomputeran awan ditamatkan.

1.23.3 Pengurusan Perubahan Perkhidmatan Pengkomputeran Awan	**Tanggungjawab**
Pengurusan perubahan perlu dilaksanakan berdasarkan perkara berikut: a) pertukaran infrastruktur yang mengubah perkhidmatan yang ditawarkan dalam pengkomputeran awan; b) penyimpanan atau pemprosesan maklumat mengikut pemetaan geografi yang baharu mengikut undang-undang; dan c) penyedia melantik syarikat lain sebagai pengendali perkhidmatan pengkomputeran awan.	ICTSO Pengurus ICT Pentadbir Pusat Data

1.24 Perancangan dan Penyediaan Pengurusan Insiden Keselamatan Maklumat

Objektif

Memastikan perancangan pengurusan insiden keselamatan maklumat yang dilaksanakan adalah konsisten dan teratur.

1.24.1 Tugas dan Tanggungjawab	**Tanggungjawab**
Perkara yang perlu diambil kira adalah seperti yang berikut: a) mewujudkan prosedur bagi mengendalikan pengurusan insiden keselamatan maklumat;	ICTSO Pengurus ICT CSIRT JPA

b) memastikan tindakan pengukuhan serta maklum balas yang cepat, efektif dan teratur bagi setiap insiden keselamatan maklumat;
c) pemakluman kepada agensi kerajaan pusat yang bertanggungjawab dalam menangani insiden keselamatan; dan
d) menyediakan latihan yang bersesuaian kepada pasukan teknikal yang bertanggungjawab ke atas insiden keselamatan.

1.24.2 Prosedur Pengurusan Insiden	Tanggungjawab
Perkara yang perlu diambil kira seperti yang berikut: a) penilaian risiko ke atas insiden yang berlaku; b) pemantauan, pengelasan, analisis dan laporan insiden perlu disediakan sama ada secara manual atau melalui sistem; c) memastikan log aktiviti insiden keselamatan direkodkan; dan d) mengenal pasti punca insiden.	ICTSO Pengurus ICT CSIRT JPA

1.25 Penilaian dan Tindakan Insiden Keselamatan Maklumat

Objektif

Mengenal pasti kategori dan penilaian berasaskan keutamaan ke atas semua insiden keselamatan maklumat.

Penilaian dan Tindakan Insiden Keselamatan Maklumat	Tanggungjawab
Aktiviti keselamatan maklumat hendaklah dinilai dan dianalisis untuk diklasifikasikan sebagai insiden keselamatan maklumat. Perkara yang perlu diambil kira adalah seperti yang berikut: a) mengenal pasti dan mengesahkan kategori serta keutamaan insiden maklumat; dan b) merekodkan dan menyimpan semua tindakan serta keputusan insiden keselamatan maklumat untuk tujuan rujukan masa hadapan.	ICTSO Pengurus ICT

1.26 Tindak Balas Terhadap Insiden Keselamatan Maklumat

Objektif

Melaksanakan tindak balas yang cepat dan berkesan terhadap insiden keselamatan maklumat.

Tindak Balas Pada Insiden Keselamatan Maklumat	Tanggungjawab
Perkara yang perlu diambil kira adalah seperti yang berikut: a) mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; b) melaksanakan kajian dan analisis; c) menghubungi pihak berkuasa atau agensi yang berkenaan dengan secepat mungkin; d) menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; e) menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; f) menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan sekiranya perlu; g) menyediakan tindakan pemulihan (restoration) dengan kadar segera; h) menangani insiden keselamatan maklumat berdasarkan peraturan yang berkuat kuasa; i) insiden perlu ditutup secara rasmi dan direkodkan setelah insiden berjaya ditangani; dan j) melaksanakan pascainsiden untuk mengenal pasti punca insiden.	ICTSO CSIRTJPA

1.27 Penambahbaikan Kawalan daripada Insiden Keselamatan Maklumat yang Lepas

Objektif

Meningkatkan kawalan keselamatan berdasarkan analisis dan penyelesaian insiden keselamatan maklumat yang telah dilaksanakan bagi mengelakkan insiden yang sama berulang.

Pengajaran dari insiden keselamatan maklumat yang lepas	Tanggungjawab
Penilaian insiden yang perlu diambil kira adalah seperti yang berikut: a) menambah baik pelan pengurusan insiden;	ICTSO CSIRTJPA

b) mengenal pasti punca insiden yang kerap berlaku bagi melaksanakan kawalan tambahan yang diperlukan untuk mengurangkan risiko; dan
c) meningkatkan kesedaran keselamatan maklumat kepada warga JPA.

1.28 Pengumpulan Bukti

Objektif

Memastikan pengurusan penyimpanan bukti direkodkan secara konsisten bagi insiden keselamatan maklumat untuk tindakan tatatertib dan undang-undang.

Pengumpulan dan Pengendalian Bukti	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti berikut: a) mengenal pasti, mengumpul, menyimpan dan melindungi bahan bukti untuk mengelakkan pengubahsuaian tanpa kebenaran; b) menyimpan jejak audit, *back up* secara berkala dan melindungi integriti bahan bukti; dan c) sistem maklumat perlu merekodkan semua bukti insiden selaras dengan tarikh dan masa kejadian.	ICTSO CSIRTJPA

1.29 Keselamatan Maklumat Semasa Gangguan

Objektif

Memastikan perancangan untuk melindungi perkhidmatan dan maklumat dilindungi semasa berlakunya gangguan.

1.29.1 Perancangan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	Tanggungjawab
Perkara berikut perlu diberi perhatian: a) membangunkan Pelan Pengurusan Kesinambungan Perkhidmatan (PKP) dengan mengenal pasti aspek keselamatan maklumat yang terlibat; b) memastikan keselamatan maklumat dan perkhidmatan sistem maklumat dilindungi semasa gangguan bencana; c) mengaktifkan PKP mengikut tempoh yang ditetapkan; d) memastikan tiada gangguan kepada proses dalam penyediaan perkhidmatan JPA; dan e) memastikan pelan ini diluluskan oleh pegawai yang bertanggungjawab.	Pasukan PKP

1.29.2 Pelaksanaan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	Tanggungjawab
Perkara yang perlu diambil kira adalah seperti yang berikut: a) mengenal pasti aspek keselamatan maklumat dalam membangunkan pelan kesinambungan perkhidmatan; b) mengenal pasti aset, tanggungjawab, struktur JPA dan menetapkan prosedur pemulihan yang bersesuaian; c) mengenal pasti ancaman yang boleh mengakibatkan gangguan terhadap proses perkhidmatan JPA; d) mengenal pasti kemungkinan dan impak gangguan tersebut serta akibatnya terhadap keselamatan ICT; e) menjalankan analisis impak JPA; f) melaksanakan prosedur keselamatan bagi membolehkan pemulihan dapat dilaksanakan dalam jangka masa yang ditetapkan; g) merekodkan proses dan prosedur yang telah ditetapkan; h) mengadakan program latihan secara berkala kepada warga JPA mengenai prosedur kecemasan; i) membuat *backup* mengikut prosedur yang ditetapkan; dan j) menguji, menyelenggara dan mengemas kini setiap pelan dalam PKP mengikut keperluan.	Pasukan PKP
1.29.3 Mengkaji, Menilai dan Mengesahkan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	**Tanggungjawab**
Perkara yang perlu diambil kira adalah seperti yang berikut: a) senarai aktiviti teras dan aset yang dianggap kritikal mengikut susunan keutamaan; b) senarai warga JPA dan Pihak Luaran berserta maklumat perhubungan (nombor telefon dan alamat e-mel); c) alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah terancam; d) menetapkan arahan pemulihan maklumat dan kemudahan yang berkaitan; e) perjanjian dengan Pihak Luaran untuk mendapatkan penyambungan semula perkhidmatan mengikut keutamaan; f) salinan pelan kesinambungan perkhidmatan perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama; g) pelan kesinambungan perkhidmatan hendaklah diuji secara berkala atau apabila terdapat perubahan dalam persekitaran atau fungsi JPA untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala	CDO Pasukan PKP

hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan; dan

h) ujian pelan hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab serta peranan mereka apabila pelan dilaksanakan.

1.30 Ketersediaan ICT bagi Kesinambungan Perkhidmatan

Objektif

Memastikan ketersediaan maklumat dan aset ICT yang berkaitan semasa gangguan berdasarkan Pelan Pemulihan Bencana (PPB).

1.30.1 Pengenalpastian Ketersediaan aset ICT Semasa Gangguan	Tanggungjawab
Perkara yang perlu diambil kira adalah seperti berikut: a) mengenal pasti *Recovery Time Objective* (RTO) dan *Recovery Point Objective* (RPO) untuk sistem aplikasi kritikal mengikut keutamaan; b) menyediakan Pelan Pemulihan Bencana ICT (PPB) dan memastikan pelan ini diluluskan oleh pegawai yang bertanggungjawab; c) menjalankan pengujian bagi memastikan ketersediaan aset ICT dapat berfungsi semasa gangguan; dan d) senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya.	Pasukan *DRP*

1.31 Keperluan Undang-undang, Peraturan dan Kontrak

Objektif

Bagi memastikan pematuhan kepada keperluan undang-undang yang berkaitan dengan keselamatan maklumat. Semua keperluan undang-undang berkanun, peraturan dan kontrak perjanjian yang berkaitan dengan JPA perlu ditakrifkan, didokumenkan, dan disimpan sehingga tarikh yang sesuai bagi setiap sistem maklumat.

1.31.1 Pengenalpastian Keperluan Perundangan dan Perjanjian Kontrak	Tanggungjawab
Pihak Luaran (Pihak Kontraktor/ Perunding) yang melanggar mana-mana klausa dalam *integrity pact* boleh ditamatkan perkhidmatannya. Senarai perundangan dan peraturan yang berkuat kuasa dari semasa ke semasa perlu dipatuhi oleh semua warga JPA adalah seperti di **LAMPIRAN 3**.	Pihak Luaran

1.31.2 Kawalan Kriptografi	Tanggungjawab
Kunci enkripsi mestilah dilindungi dengan menggunakan cara kawalan yang terbaik dan hendaklah dirahsiakan. Semua kunci mestilah dilindungi daripada pengubahsuaian, pemusnahan dan sebaran tanpa kebenaran sepanjang kitaran hayat kunci tersebut. Kunci enkripsi mestilah dilindungi dengan menggunakan cara kawalan yang terbaik dan hendaklah dirahsiakan. Semua kunci mestilah dilindungi daripada pengubahsuaian, pemusnahan dan sebaran tanpa kebenaran sepanjang kitaran hayat kunci tersebut. Kriptografi turut merangkumi kaedah-kaedah seperti yang berikut: a) kesemua pelaksanaan sistem hendaklah menggunakan ID atau kata laluan dan dibuat enkripsi; dan b) penggunaan *Public Key Infrastructure* (PKI) yang selamat yang dibekalkan oleh Kerajaan.	Pentadbir Sistem Aplikasi Pengguna

1.32 Hak Harta Intelek

Objektif

Bagi memastikan pematuhan ke atas undang-undang terhadap harta intelek.

Pematuhan Terhadap Hak Harta Intelek (Intellectual Property Rights)	Tanggungjawab
Warga JPA dan Pihak Luaran perlu mengiktiraf dan menghormati hak-hak harta intelek yang berkaitan dengan sistem maklumat. Warga JPA dan pihak Luaran hendaklah mematuhi: a) keperluan hak cipta yang berkaitan dengan bahan *proprietary*, perisian, dan reka bentuk yang diperoleh melalui JPA; b) keperluan pelesenan mengehadkan penggunaan produk, perisian, reka bentuk dan bahan-bahan lain yang diperoleh oleh JPA;	Warga JPA Pihak Luaran

c) pematuhan yang berterusan dengan sekatan hak cipta produk dan keperluan pelesenan; dan
d) pengguna tidak dibenarkan menggunakan kemudahan pemprosesan maklumat bagi tujuan yang tidak dibenarkan.

1.33 Perlindungan Rekod

Objektif

Bagi memastikan pematuhan ke atas undang-undang yang berkaitan dengan rekod.

Perlindungan Rekod	Tanggungjawab
Rekod-rekod yang penting (fizikal atau digital) hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, capaian yang tidak dibenarkan, penyebaran yang tidak dibenarkan mengikut undang-undang, peraturan, kontrak, dan keperluan perniagaan Perkara yang perlu dipertimbangkan ialah: a) pengekalan, penyimpanan, pengendalian dan pelupusan rekod dan maklumat; b) jadual penyimpanan rekod perlu dikenal pasti; dan c) inventori rekod.	Warga JPA Pihak Luaran

1.34 Privasi dan Perlindungan Maklumat Peribadi

Objektif

Bagi memastikan pematuhan ke atas undang-undang yang berkaitan dengan aspek Keselamatan maklumat peribadi.

Perlindungan dan Privasi Data Peribadi	Tanggungjawab
Privasi dan perlindungan maklumat peribadi pengguna dijamin seperti yang tertakluk dalam undang-undang kerajaan Malaysia dan peraturan-peraturan yang berkenaan.	ICTSO

1.35 Kajian oleh Pihak Bebas / Luaran Berkaitan Keselamatan Maklumat

Objektif

Bagi memastikan pendekatan yang digunakan oleh JPA bersesuaian, cukup dan berkesan secara lebih efektif.

Kajian Bebas/ Pihak Luaran Terhadap Keselamatan Maklumat	Tanggungjawab
Pelaksanaan keselamatan maklumat JPA hendaklah dikaji secara bebas atau oleh Pihak Luaran pada jangka masa yang dirancang atau apabila perubahan ketara berlaku dalam pelaksanaannya.	Jawatankuasa Pelaksana ISMS Audit SIRIM

1.36 Piawaian untuk Keselamatan Maklumat

Objektif

Memastikan keselamatan maklumat dilaksanakan mengikut polisi keselamatan maklumat serta piawaian dan peraturan semasa.

1.36.1 Pematuhan Dasar dan Standard/ Piawaian	Tanggungjawab
JPA hendaklah membuat kajian semula pematuhan berdasarkan standard/ piawaian yang berkaitan. Sekiranya kajian semula mendapati berlaku ketidakpatuhan, JPA perlu: a) mengenal pasti punca ketidakpatuhan; b) menilai keperluan tindakan untuk mencapai pematuhan; c) melaksanakan tindakan pembetulan yang sewajarnya; dan d) mengkaji semula tindakan pembetulan yang diambil untuk mengesahkan keberkesanannya dan mengenal pasti apa-apa kekurangan dan kelemahan.	Pengurus ICT
1.36.2 Penilaian Tahap Keselamatan	**Tanggungjawab**
Sistem maklumat hendaklah diuji selaras dengan pematuhan peraturan semasa yang berkuat kuasa. Penilaian ini perlu dilaksanakan sekurang-kurangnya sekali dalam setahun atau mengikut keperluan.	ICTSO Pentadbir Sistem Pentadbir Rangkaian dan Keselamatan Pentadbir Pusat Data

1.37 Prosedur Operasi yang Perlu Didokumenkan

Objektif

Prosedur operasi bagi kemudahan pemprosesan maklumat perlu disediakan dan dapat diakses dengan selamat.

1.37.1 Penyediaan Prosedur Operasi	Tanggungjawab
Menyediakan dokumen operasi standard untuk perkara berikut: a) aktiviti yang sentiasa dilaksanakan oleh Warga JPA; b) aktiviti yang jarang dilaksanakan; c) aktiviti yang baharu dan penilaian risiko tidak dapatkan dijalankan dengan betul; dan d) serahan tugas kepada kakitangan baharu.	ICTSO Pentadbir Sistem Aplikasi

1.37.2 Kandungan Dokumen Prosedur Operasi	Tanggungjawab
Dokumen Prosedur Operasi hendaklah diwujudkan, disemak dan dikemas kini mengikut keperluan. Kandungan dokumen yang perlu disediakan adalah seperti yang berikut: a) pegawai bertanggungjawab; b) instalasi dan konfigurasi sistem; c) pemprosesan maklumat secara manual dan automatik; d) sandaran (backup); e) jadual keperluan termasuk kebergantungan dengan sistem lain; f) pengendalian ralat; g) khidmat sokongan sekiranya berlaku masalah operasi dan teknikal; h) arahan pengendalian media storan; i) prosedur pemulihan sekiranya berlaku kegagalan sistem; j) pengurusan jejak audit sistem; k) pemantauan ke atas kapasiti prestasi dan keselamatan sistem; dan l) manual penyelenggaraan.	ICTSO Pentadbir Sistem Aplikasi

BAB 2

KAWALAN MANUSIA

2.1 Tapisan Keselamatan Individu

Objektif

Memastikan kakitangan dan orang awam memahami tanggungjawab serta peranan dalam aspek keselamatan ICT sepanjang tempoh perkhidmatan mereka.

2.1.1 Tapisan ke atas Kakitangan Awam (Tapisan Sebelum Pengesahan Pelantikan)	Tanggungjawab
Pengesahan pelantikan perlu mengambil kira perkara seperti yang berikut: a) memeriksa kesahihan maklumat yang merangkumi identiti pengenalan diri, rujukan individu, *resume,* kelayakan akademik, sijil profesional dan rekod jenayah; b) menjalankan tapisan keselamatan untuk pegawai dan kakitangan yang terlibat. Ia berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; c) mengehadkan capaian dan penggunaan aset kerajaan; dan d) mengambil tindakan seperti menangguhkan pelantikan atau membatalkan pelantikan sekiranya kakitangan tidak melepasi tapisan dalam tempoh yang ditetapkan.	ICTSO Pengurus ICT

2.1.2 Tapisan ke atas Pihak Luaran	Tanggungjawab
Tapisan ke atas perkara-perkara berikut: a) memeriksa kesahihan maklumat yang merangkumi identiti pengenalan diri, surat tawaran kerja serta perkara lain yang berkaitan serta bersesuaian dengan tawaran kerja yang diberikan; b) memastikan semua pekerja menjalani tapisan keselamatan berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; c) mengehadkan capaian dan penggunaan aset kerajaan; dan d) mengambil tindakan seperti menangguhkan pelantikan atau membatalkan pelantikan individu yang tidak melepasi tapisan dalam tempoh yang ditetapkan.	ICTSO Pengurus ICT Pihak Luaran

2.2 Terma dan Syarat Pelantikan

Objektif

Memastikan kakitangan dan Pihak Luaran memahami tanggungjawab serta peranan dalam keselamatan ICT.

Terma dan Syarat Pelantikan	Tanggungjawab
Terma dan Syarat Pelantikan yang perlu dipatuhi adalah seperti yang berikut: a) mengisi dan memperakui pematuhan perjanjian melalui Surat Akuan Pematuhan Polisi Keselamatan Siber (PKS) JPA atau Perakuan Untuk Ditandatangani oleh Komuniti Keselamatan Atau Mana-mana Pihak Lain Yang Berurusan Dengan Perkhidmatan Awam atau Yang Berkhidmat di Kediaman Rasmi Kerajaan Berkaitan Dengan Akta Rahsia Rasmi 1972 (Akta 88) bagi tujuan menjaga kerahsiaan maklumat dan aset ICT yang berkaitan; b) memahami dan bersetuju ke atas tanggungjawab serta hak berkaitan perlindungan keselamatan maklumat; c) memahami peranan dan tanggungjawab dalam keselamatan penyampaian maklumat bagi mengurangkan risiko penyalahgunaan aset ICT; d) mematuhi semua terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan dan ditandatangani; e) bertanggungjawab untuk mengklasifikasikan maklumat dan aset lain yang berkaitan; f) bertanggungjawab untuk mengendali maklumat daripada pihak berkepentingan; dan g) bertanggungjawab untuk mengambil tindakan jika keselamatan maklumat tidak dipatuhi.	ICTSO Pengurus ICT Warga JPA Pihak Luaran

2.3 Program Kesedaran, Pendidikan dan Latihan Berkaitan Keselamatan Maklumat

Objektif

Memastikan Warga JPA dan Pihak Luaran mengambil maklum dan jelas berkaitan tanggungjawab ke atas keselamatan maklumat.

2.3.1 Program Kesedaran Keselamatan Maklumat	Tanggungjawab
Perkara-perkara yang perlu dilaksanakan adalah seperti yang berikut: a) mendapatkan sokongan pengurusan atasan berkaitan keselamatan maklumat; b) memberikan kesedaran berkaitan undang-undang, peraturan dan perjanjian; c) melaksanakan program kesedaran berkaitan dengan keselamatan maklumat kepada warga JPA dan Pihak Luaran secara berterusan semasa melaksanakan tugas-tugas dan tanggungjawab mereka; dan d) memaklumkan senarai perhubungan sekiranya pelanggaran maklumat dikesan oleh warga JPA atau Pihak Luaran.	ICTSO Pengurus ICT

2.3.2 Program Latihan dan Pendidikan berkaitan Keselamatan Maklumat	Tanggungjawab
Perkara-perkara berikut hendaklah diberi perhatian: a) mengenal pasti, menyediakan dan menjalankan latihan berkaitan keselamatan maklumat yang bersesuaian dan terkini untuk meningkatkan kemahiran bagi memastikan keselamatan maklumat di tahap yang optimum; b) memastikan latihan dan program kesedaran yang diberikan kepada pengguna dari semasa ke semasa bagi meningkatkan kompetensi pengguna berkaitan keselamatan maklumat; dan c) memastikan prosedur latihan jabatan sentiasa dikemas kini bersesuaian dengan fungsi tugas semasa setiap pengguna.	Pengurus ICT

2.4 Tindakan Disiplin

Objektif

Memastikan kakitangan dan Pihak Luaran memahami kesan pelanggaran ke atas keselamatan maklumat mengikut undang-undang atau peraturan lain-lain yang sedang berkuat kuasa.

Tindakan Pelanggaran Undang-undang dan Peraturan	Tanggungjawab
Tindakan boleh dikenakan ke atas kakitangan dan Pihak Luaran yang tidak mematuhi keselamatan maklumat. Langkah-langkah yang perlu diambil adalah: a) memastikan adanya proses tindakan perundangan ke atas Pihak Luaran sekiranya berlaku pelanggaran terhadap Akta Rahsia Rasmi 1972 (Akta 88); dan b) memastikan adanya proses tindakan tatatertib ke atas warga JPA sekiranya berlaku pelanggaran terhadap Peraturan-Peraturan Pegawai Awam (Kelakuan dan Tatatertib) 1993 [P.U.(A) 395/1993], dasar-dasar Kerajaan, undang-undang serta peraturan yang berkuat kuasa.	Pengurus ICT Penasihat Undang-Undang Ketua Unit Integriti Warga JPA Pihak Luaran

2.5 Tanggungjawab Selepas Pertukaran atau Penamatan Kerja

Objektif

Melindungi kepentingan jabatan semasa proses pertukaran atau penamatan warga JPA.

Penamatan atau Pertukaran	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) memastikan semua aset ICT dikembalikan kepada JPA mengikut peraturan dan terma perkhidmatan yang ditetapkan; b) melaksanakan pertukaran atau penamatan hendaklah ditakrifkan dengan jelas termasuk: i. perubahan dalam terma dan syarat pertukaran atau penamatan tanggungjawab; ii. tempoh akhir pekerjaan; dan iii. tanggungjawab masih sah selepas penamatan. c) menjaga kerahsiaan keselamatan maklumat walaupun selepas penamatan atau pertukaran; dan d) membatalkan atau menarik balik semua kebenaran hak akses ke atas sistem maklumat mengikut peraturan yang ditetapkan.	ICTSO Pengurus ICT Warga JPA Pihak Luaran

2.6 Perjanjian Kerahsiaan atau *Non-Disclosure Agreement*

Objektif

Memastikan kerahsiaan maklumat yang boleh diakses oleh warga JPA atau Pihak Luaran dikenal pasti, didokumenkan, disemak secara berkala dan ditandatangani.

Kerahsiaan atau *Non-Disclosure Agreement*	**Tanggungjawab**
Perjanjian kerahsiaan perlu melindungi maklumat berdasarkan undang-undang yang berkuat kuasa terhadap pihak yang berkepentingan dan warga JPA. Kandungan *Non-Disclosure Agreement* yang perlu dipatuhi adalah seperti yang berikut: a) definisi maklumat yang perlu dilindungi; b) tempoh perjanjian kerahsiaan; c) tindakan selepas penamatan perjanjian; d) pengesahan ke atas peminjaman atau akses maklumat perlu dilaksanakan bagi mencegah kebocoran maklumat; e) pemilikan maklumat, kerahsiaan dan harta intelek yang berkaitan dengan perlindungan kerahsiaan maklumat; f) kebenaran untuk menggunakan maklumat rahsia rasmi; g) hak untuk mengaudit dan memantau aktiviti yang melibatkan maklumat rahsia rasmi; h) proses pemakluman dan pelaporan kebocoran atau pendedahan maklumat; i) syarat pemulangan atau penghapusan maklumat selepas perjanjian tamat; dan j) tindakan undang-undang sekiranya perjanjian tidak dipatuhi.	ICTSO Pihak Luaran

2.7 Bekerja Jarak Jauh

Objektif

Memastikan kawalan keselamatan terhadap individu yang bekerja jarak jauh untuk melindungi keselamatan maklumat.

2.7.1 Kerja Jarak Jauh	**Tanggungjawab**
Kebenaran aktiviti kerja jarak jauh di luar premis JPA perlu mematuhi perkara seperti yang berikut: a) keselamatan fizikal bagi lokasi bekerja jarak jauh seperti di rumah atau lokasi yang dibenarkan sahaja; b) kawalan keselamatan yang merangkumi kabinet fail berkunci, peraturan berkaitan *remote access, clear desk*,	Pengurus ICT Warga JPA Pihak Luaran

pencetakan dan pelupusan maklumat atau aset lain yang berkaitan dan insiden keselamatan;

c) mengenal pasti lokasi persekitaran fizikal untuk bekerja jarak jauh;
d) menggunakan kawalan komunikasi yang selamat untuk akses ke atas maklumat rahsia rasmi, sistem dan aplikasi kritikal;
e) membenarkan peralatan milik persendirian digunakan untuk *remote access* seperti perisian *Remote Desktop*;
f) mengehadkan konfigurasi rangkaian tanpa wayar (Wi-Fi) dengan membuat pemilihan kategori rangkaian yang selamat;
g) penggunaan kawalan peralatan atau perisian keselamatan; dan
h) pengesahan dan pengaktifan hak akses jarak jauh yang selamat semasa menggunakan rangkaian luar JPA.

2.7.2 Garis Panduan Kerja Jarak Jauh	**Tanggungjawab**
Garis panduan kerja jarak jauh hendaklah mematuhi perkara berikut: a) menetapkan klasifikasi maklumat dan perkhidmatan sistem yang boleh diakses oleh individu bekerja jarak jauh; b) memastikan keselamatan fizikal; c) menyediakan peraturan serta panduan akses peralatan dan maklumat oleh pihak lain; d) melaksanakan prosedur sandaran dan kesinambungan perkhidmatan; dan e) membatalkan hak akses dan pemulangan peralatan apabila aktiviti kerja jarak jauh selesai.	Pentadbir Rangkaian dan Keselamtaan Warga JPA Pihak Luaran

2.8 Pelaporan Insiden Keselamatan Maklumat

Objektif

Memastikan insiden dikendalikan dengan berkesan bagi meminimumkan impak supaya tidak menjejaskan sistem penyampaian perkhidmatan.

Pelaporan Insiden Keselamatan Maklumat	Tanggungjawab
Insiden keselamatan merangkumi insiden, pelanggaran dan kerentanan sistem. Warga JPA dan Pihak Luaran yang menggunakan sistem dan perkhidmatan maklumat JPA dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT. Insiden keselamatan perlu dilaporkan apabila berlaku perkara seperti yang berikut: a) kawalan keselamatan maklumat yang tidak berkesan; b) pelanggaran sebarang kerahsiaan, integriti atau ketersediaan maklumat; c) kesilapan manusia; d) ketidakpatuhan terhadap polisi keselamatan maklumat; pelanggaran keselamatan fizikal; e) perubahan sistem yang tidak melalui proses pengurusan perubahan; f) perisian atau perkakasan yang rosak atau tidak berfungsi; g) penyalahgunaan hak akses; h) kerentanan; dan i) percubaan serangan perisian hasad.	CSIRT JPA Pengurus ICT Warga JPA Pihak Luaran

BAB 3

KAWALAN FIZIKAL

3.1 Perimeter Keselamatan Fizikal

Objektif

Memastikan kawalan keselamatan fizikal berkaitan maklumat, premis dan kemudahan ICT.

Keselamatan Fizikal	Tanggungjawab
Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh premis. Langkah-langkah keselamatan fizikal adalah seperti yang berikut: a) menetapkan perimeter kawasan keselamatan fizikal dan keperluan keselamatan bagi melindungi aset yang berkaitan; b) memastikan perimeter kawasan yang dilindungi atau mempunyai kemudahan pemprosesan maklumat dikawal menggunakan pagar kawalan, pengawal keselamatan, sistem kad akses, dinding konkrit dan kawalan yang bersesuaian; c) memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; d) memastikan kawalan kunci dengan menetapkan pegawai yang bertanggungjawab untuk menyimpan kunci dengan baik dan mempunyai rekod; e) memasang dan menguji alat penggera kebakaran; f) memasang dan memantau sistem CCTV; g) mengadakan kaunter kawalan; h) menyediakan tempat atau bilik khas untuk Pihak Luaran; i) mereka bentuk dan melaksanakan perlindungan fizikal daripada bencana; j) menyediakan garis panduan keselamatan untuk warga JPA yang bekerja di dalam kawasan terhad; dan k) mewujudkan kawalan di kawasan penghantaran, pemunggahan dan kawasan larangan.	Pengurus ICT Warga JPA

3.2 Kawalan Kemasukan Fizikal

Objektif

Melaksanakan kawalan akses masuk kepada maklumat, premis dan kemudahan ICT.

3.2.1 Kawalan Akses Masuk Fizikal	Tanggungjawab
Kawalan keluar masuk ke premis JPA seperti kawasan penghantaran, pemunggahan dan kawasan larangan perlu mematuhi perkara seperti yang berikut: a) mengehadkan akses masuk ke kawasan yang berkaitan kepada kakitangan yang dibenarkan sahaja berdasarkan kelulusan; b) menyediakan dan menyemak buku log *audit trail* akses ke pusat data secara berkala; c) menggunakan kad akses untuk kemasukan fizikal ke kawasan penyimpanan maklumat atau kawasan larangan; d) menyediakan kawasan menunggu atau penerimaan yang boleh dipantau oleh pegawai bertanggungjawab JPA; e) melaksanakan pemeriksaan fizikal kepada pengguna dan barangan kepunyaan peribadi; f) memastikan pemakaian pas keselamatan sepanjang berada di premis JPA; g) memberikan akses yang terhad dan pemantauan kepada kakitangan Pihak Luaran ke kawasan pemprosesan maklumat atau kawasan larangan apabila diperlukan sahaja; h) memastikan keselamatan akses ke atas peralatan JPA yang ditempatkan di lokasi berkongsi dengan agensi lain; i) mengemas kini kawalan keselamatan fizikal dengan lebih kukuh bagi insiden yang kerap berlaku atau meningkat; j) memastikan pintu masuk lain seperti pintu kecemasan dikawal daripada akses tanpa kebenaran; dan k) menetapkan proses pengurusan kunci bagi memastikan kunci fizikal atau kod berkunci ke kawasan pemprosesan maklumat atau kawasan larangan dipantau dan direkodkan.	ICTSO Pengurus ICT Warga JPA Pihak Luaran

3.2.2 Kawalan Keselamatan Pelawat	Tanggungjawab
Perkara berikut perlu dipatuhi: a) setiap pelawat mestilah mendaftar dan mendapatkan pas pelawat di pintu masuk utama; b) mengesahkan identiti pelawat, memaparkan pas pelawat sepanjang di premis dan mengembalikan pas pelawat selepas selesai urusan; c) merekodkan maklumat keluar dan masuk pelawat; d) hanya memberikan kebenaran akses kepada kawasan yang diperlukan sahaja; e) pelawat perlu diiringi oleh warga JPA di kawasan yang berkaitan; dan f) kehilangan pas keselamatan mestilah dilaporkan dengan segera kepada pegawai keselamatan JPA.	ICTSO Pengurus ICT

3.2.3 Kawasan Penghantaran dan Pemunggahan	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) mempunyai akses terhad kepada kawasan penghantaran dan pemunggahan oleh Pihak Luaran; b) memastikan Pihak Luaran tidak dibenarkan masuk ke lokasi lain tanpa kebenaran; c) memastikan kawasan penghantaran dan pemunggahan atau tempat lain dikawal semasa proses penghantaran dan pemunggahan; d) memeriksa dan memastikan barang yang dihantar tidak mengandungi bahan letupan atau bahan berbahaya yang lain; e) semua penghantaran barang perlu didaftar mengikut prosedur pengurusan aset; dan f) memastikan barang yang diterima tidak diubah suai tanpa kebenaran.	ICTSO Pengurus ICT

3.3 Keselamatan Pejabat, Bilik dan Kemudahan ICT

Objektif

Memastikan keselamatan dan perlindungan daripada sebarang bentuk pencerobohan, ancaman, kerosakan, kecuaian serta akses yang tidak dibenarkan.

Kawalan Pejabat, Bilik dan Kemudahan ICT	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) memastikan kawasan larangan dihadkan daripada akses tanpa kebenaran; b) memastikan penunjuk ke lokasi bilik operasi atau kawasan larangan tidak didedahkan atau hanya memberi petunjuk yang minimum; c) memastikan maklumat kawasan larangan tidak dapat dilihat oleh Pihak Luaran; dan d) memastikan maklumat perhubungan atau lokasi kawasan larangan tidak didedahkan tanpa kebenaran.	ICTSO Pengurus ICT Warga JPA

3.4 Pemantauan Keselamatan Fizikal

Objektif

Memantau dan memastikan keselamatan fizikal dikawal.

Pemantauan Terhadap Premis Fizikal	Tanggungjawab
Pemantauan kepada bangunan yang menempatkan sistem kritikal perlu dipantau dengan cara berikut: a) memasang dan memantau sistem kamera litar tertutup (CCTV) di dalam dan luar bangunan JPA; b) mengehadkan akses berdasarkan peranan dan tanggungjawab individu melalui Sistem Pengurusan Kad Akses dan/atau Biometrik; c) memastikan pemasangan penggera yang merangkumi semua pintu yang boleh akses masuk ke kawasan larangan; dan d) reka bentuk sistem pemantauan tidak boleh didedahkan tanpa kebenaran untuk mengelakkan kebocoran maklumat dan di pecah masuk.	Pengurus ICT

3.5 Perlindungan Terhadap Ancaman Fizikal dan Bencana Alam

Objektif

Memastikan infrastruktur yang direka bentuk dilindungi daripada ancaman fizikal dan bencana alam.

Perlindungan Terhadap Ancaman Fizikal dan Bencana Alam	Tanggungjawab
Penilaian risiko ke atas ancaman fizikal dan bencana alam perlu dijalankan secara berkala. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) mereka bentuk dan melaksanakan pelan perlindungan fizikal daripada kebakaran dan bencana alam; b) memastikan pelan tindakan perlindungan bagi ancaman berbahaya seperti letupan, kacau-bilau, rusuhan dan sebagainya; dan c) pelan tindakan perlindungan perlu merangkumi kawalan seperti bencana alam, kebakaran, gangguan bekalan elektrik dan letupan.	Pengurus ICT

3.6 Bekerja di Kawasan Larangan

Objektif

Memastikan maklumat dan aset ICT berada di kawasan yang selamat daripada gangguan atau kerosakan daripada pekerja sekitarnya.

Kawasan Larangan	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) memastikan individu yang bekerja di kawasan tersebut memahami tanggungjawab mereka; b) memantau dan mengawasi setiap kerja yang dijalankan di kawasan larangan; c) kawasan larangan perlu sentiasa berkunci dan memeriksa ruangan kosong yang ada; d) fotografi, video, audio dan peralatan rakaman lain tidak dibenarkan dibawa masuk melainkan dengan kebenaran; e) mengawal peranti yang dibenarkan dibawa masuk ke dalam kawasan larangan; dan f) memaparkan prosedur kecemasan yang mudah dilihat atau diakses.	Pengurus ICT Warga JPA Pihak Luaran

3.7 *Clear Desk and Clear Screen*

Objektif

Memastikan kawalan capaian maklumat yang tidak dibenarkan di atas meja atau di paparan skrin atau di mana-mana lokasi yang boleh diakses semasa dan di luar waktu pejabat.

Clear Desk and Clear Screen	**Tanggungjawab**
Clear Desk and Clear Screen bermaksud tidak meninggalkan maklumat sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) menggunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer; b) menetapkan paparan skrin akan tertutup selepas 10 minit tidak digunakan oleh pengguna; c) dokumen terperingkat hendaklah disimpan dalam laci atau kabinet fail yang berkunci; d) membersihkan maklumat sensitif atau kritikal pada papan putih dan jenis paparan lain apabila tidak diperlukan lagi; e) memastikan semua dokumen diambil segera dari pencetak, pengimbas dan mesin fotostat; dan f) menghalang penggunaan tanpa kebenaran mesin fotostat dan teknologi penghasilan semula seperti mesin pengimbas atau kamera digital.	Warga JPA

3.8 Penempatan dan Perlindungan aset ICT

Objektif

Memastikan aset ICT ditempatkan di kawasan yang selamat dan dilindungi daripada sebarang bentuk pencerobohan dan ancaman.

Penempatan dan Perlindungan aset ICT	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) kemudahan penyimpanan perlu dilindungi untuk menghalang akses yang tidak dibenarkan; b) kemudahan pemprosesan maklumat yang melaksanakan pengendalian maklumat rahsia rasmi harus ditempatkan dengan teliti untuk mengurangkan risiko maklumat tersebut dapat dilihat oleh pihak yang tidak berkaitan;	ICTSO Pengurus ICT Warga JPA Pihak Luaran

c) mengadaptasi kawalan untuk mengurangkan risiko potensi ancaman fizikal dan bencana alam seperti kecurian, kebakaran, gangguan bekalan elektrik; dan lain-lain;
d) menetapkan larangan makan, minum dan merokok di kedudukan berhampiran dengan kemudahan pemprosesan maklumat;
e) pemantauan terhadap keadaan persekitaran seperti suhu dan kelembapan serta keadaan yang boleh menjejaskan operasi kemudahan pemprosesan maklumat;
f) pemasangan alat perlindungan kilat;
g) peralatan yang memerlukan perlindungan khas perlu dilindungi daripada bahaya atau kerosakan dengan langkah yang sesuai;
h) sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; dan
i) sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada Pengurus ICT.

3.9 Keselamatan Aset di Luar Pejabat

Objektif

Memastikan keselamatan aset ICT yang dibawa keluar dari premis dilindungi.

Peralatan ICT di Luar Premis	Tanggungjawab
Semua peralatan aset ICT JPA yang digunakan di luar pejabat perlu mendapatkan kelulusan terlebih dahulu. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) tidak meninggalkan peralatan atau media yang menyimpan maklumat rahsia rasmi di tempat awam tanpa pengawasan; b) mematuhi panduan untuk melindungi aset ICT pada setiap masa seperti terdedah kepada haba atau suhu yang tinggi; c) memastikan maklumat peminjaman atau penggunaan aset ICT/ media storan di luar pejabat direkodkan dan data rahsia rasmi dihapuskan sebelum pemulangan; d) memastikan kawalan keselamatan diambil kira semasa penggunaan aset ICT di tempat awam; e) Aset ICT yang hendak dibawa keluar dari Pejabat JPA perlu mengisi Borang Kebenaran Membawa Keluar Aset, KEW.PA-9 dan mendapatkan kelulusan daripada Pengurus ICT; dan f) mematuhi semua perkara yang dinyatakan di para 3.7.	Pengurus ICT Warga JPA Pentadbir ICT JPA

3.10 Media Storan

Objektif

Memastikan media storan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.

3.10.1 Pengurusan Media Storan Mudah Alih (Removal Media)	Tanggungjawab
Media storan digunakan untuk menyimpan data dan maklumat seperti *thumb drive, external drive* dan media storan lain. Pengendalian media storan perlu mematuhi perkara seperti yang berikut: a) media storan mudah alih hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b) memastikan media storan mudah alih boleh berfungsi sekiranya diperlukan; c) memastikan maklumat rahsia rasmi yang disimpan melebihi satu media storan mudah alih mengambil kira risiko kerosakan atau kehilangan maklumat; d) akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada Pengurus ICT dan pegawai yang dibenarkan sahaja; dan e) hanya maklumat rasmi dibenarkan untuk disimpan dalam media storan yang dibekalkan oleh JPA.	ICTSO Pengurus ICT Pentadbir ICT JPA Warga JPA

3.10.2 Keselamatan Pelupusan dan Penggunaan Semula Media	Tanggungjawab
Prosedur pelupusan dan penggunaan semula media storan hendaklah diwujudkan bagi mengurangkan risiko kebocoran maklumat. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) media storan yang akan digunakan semula perlu disanitasi atau diformat terlebih dahulu; b) melupuskan media storan yang mengandungi maklumat rahsia rasmi menggunakan kaedah yang dibenarkan sekiranya tidak diperlukan lagi; c) pelupusan media storan oleh Pihak Luaran hendaklah mematuhi kawalan keselamatan dan dilaksanakan oleh pihak yang berpengalaman; d) pelupusan maklumat mengikut Tatacara Pelupusan Arkib Negara (Akta Arkib Negara 2003 [Akta 629]); e) penghapusan maklumat atau kandungan media mestilah mendapat kelulusan;	ICTSO Pengurus ICT Pentadbir ICT JPA Warga JPA

f) pelupusan media storan hendaklah direkodkan;
g) semua media storan yang hendak dilupuskan mestilah dirujuk kepada Bahagian Digital dan Teknologi Maklumat yang bertanggungjawab berkaitan ICT; dan
h) pengguna hendaklah menghapuskan atau memindahkan semua maklumat rasmi/ terperingkat dari media storan sendiri apabila bersara/ bertukar jabatan/ ditamatkan perkhidmatan dan tamat/ ditamatkan kontrak.

3.11 Perkhidmatan Sokongan

Objektif

Memastikan kawalan ke atas perkhidmatan sokongan ICT dilindungi daripada kegagalan bekalan kuasa dan gangguan fasiliti.

Perkhidmatan Sokongan ICT	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut:	ICTSO
a) memastikan peralatan di dalam fasiliti perkhidmatan sokongan beroperasi, dikonfigurasi dan diselenggarakan mengikut spesifikasi pengeluar yang berkaitan; b) memastikan fasiliti perkhidmatan sokongan dinilai semula keupayaannya secara berkala bagi memenuhi keperluan JPA; c) memastikan peralatan sokongan disemak dan diselenggarakan dari semasa ke semasa mengikut Perjanjian Tahap Perkhidmatan (SLA); d) menyediakan fasiliti sokongan kedua; e) memastikan peralatan di dalam fasiliti perkhidmatan sokongan sentiasa disokong oleh *Uninterruptible Power Supply* (UPS); f) memastikan bekalan kuasa berterusan disalurkan kepada fasiliti sokongan seperti UPS dan penjana kuasa (*generator*) bagi membolehkan pusat data beroperasi dengan optimum supaya perkhidmatan fasiliti sokongan di pusat data mendapat bekalan kuasa berterusan; dan g) memastikan peralatan sokongan diperiksa dan diuji secara berkala oleh pihak berkaitan.	Pentadbir ICT JPA

3.12 Keselamatan Pengkabelan

Objektif

Memastikan kabel rangkaian dan kuasa elektrik dilindungi daripada gangguan dan pencerobohan.

Keselamatan Kabel	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) kabel kuasa elektrik dan rangkaian yang disambungkan ke sistem maklumat diberi perlindungan yang bersesuaian untuk mengelakkan pemotongan kabel tanpa sengaja; b) mengasingkan kabel kuasa elektrik dan rangkaian untuk mencegah gangguan penghantaran data; Memastikan kabel bagi sistem kritikal mempunyai kawalan tambahan seperti yang berikut: i. pemasangan saluran pelindung berlapis *(conduit)* dan dalam bilik berkunci; ii. semakan dan pemeriksaan teknikal secara berkala untuk mengenal pasti sambungan kabel yang tidak dibenarkan terhadap peranti; iii. kawalan akses ke bilik telekomunikasi atau bilik kabel; iv. memastikan semua sambungan kabel dilabelkan bagi membolehkan pengenalan fizikal dan pemeriksaan kabel terlibat; dan v. mendapatkan nasihat pakar berkaitan kaedah pengurusan risiko yang timbul daripada insiden atau kerosakan kabel.	ICTSO Pentadbir ICT JPA Pihak Luaran

3.13 Penyelenggaraan Peralatan

Objektif

Memastikan semua peralatan berkaitan perkhidmatan ICT diselenggarakan untuk mengelakkan gangguan operasi JPA.

Penyelenggaraan Peralatan	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) peralatan yang diselenggarakan hendaklah mematuhi spesifikasi dan tempoh penyelenggaraan yang ditetapkan oleh pengeluar; b) pemantauan pelaksanaan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan;	ICTSO Pentadbir ICT JPA Warga JPA Pihak Luaran

c) memastikan peralatan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja;
d) menyimpan rekod penyelenggaraan pencegahan dan pemulihan;
e) melaksanakan kawalan yang sesuai bagi tujuan penyelenggaraan pencegahan dan pemulihan sama ada di dalam atau luar premis JPA;
f) menyelia kerja-kerja penyelenggaraan yang dilakukan oleh Pihak Luaran;
g) mengawal akses bagi penyelenggaraan yang dilaksanakan secara jarak jauh (remote);
h) melaksanakan kawalan keselamatan ke atas penyelenggaraan peralatan di luar premis JPA;
i) menyemak dan menguji semua peralatan selepas proses penyelenggaraan bagi memastikan tiada pengubahsuaian yang tidak dibenarkan; dan
j) melaksanakan kaedah yang bersesuaian untuk pelupusan atau penggunaan semua peralatan.

3.14 Pelupusan atau Penggunaan Semula Peralatan

Objektif

Memastikan kaedah pelupusan dan penggunaan semula peralatan dilaksanakan mengikut peraturan yang berkuat kuasa.

3.14.1 Pelupusan Peralatan	Tanggungjawab
a) maklumat pelupusan hendaklah direkodkan, dikemas kini dan dilaporkan mengikut keperluan; b) warga JPA tidak dibenarkan melakukan perkara-perkara seperti berikut: i. menyimpan mana-mana peralatan yang hendak dilupuskan untuk tujuan peribadi; ii. menanggalkan komponen peralatan seperti RAM, *hard disk, motherboard* dan sebagainya; iii. melupuskan sendiri tanpa kelulusan; dan iv. memindah keluar peralatan yang dilupuskan tanpa kelulusan.	ICTSO Warga JPA Pentadbir ICT JPA

3.14.2 Penggunaan Semula Peralatan	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) semua maklumat di dalam peralatan hendaklah disanitasi atau dihapuskan secara selamat terlebih dahulu sebelum penggunaan semula atau dipindah milik; b) maklumat peralatan yang diguna semula atau dipindah milik hendaklah direkodkan dan dikemas kini; c) warga JPA tidak dibenarkan daripada melakukan perkara-perkara seperti yang berikut: i. menyimpan peralatan berlebihan untuk tujuan peribadi; ii. menanggalkan komponen peralatan seperti RAM, *hard disk, motherboard* dan sebagainya; dan iii. menggunakan semula peralatan tanpa kelulusan.	ICTSO Pentadbir ICT JPA Warga JPA

BAB 4

KAWALAN TEKNOLOGI

4.1 Aset ICT Pengguna

Objektif

Melindungi maklumat yang terdapat dalam aset ICT pengguna.

4.1.1 Pengurusan Aset ICT	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut:	ICTSO
a) memastikan jenis dan klasifikasi maklumat yang boleh diakses, diproses atau disimpan dalam aset ICT pengguna; b) memastikan semua aset ICT pengguna didaftarkan; c) memastikan pengguna bertanggungjawab ke atas aset ICT; d) memastikan perisian yang boleh dipasang pada aset ICT pengguna telah mendapat kebenaran; e) memastikan aset ICT pengguna dikonfigurasi dengan versi perisian atau *patches* terkini; f) menetapkan peraturan bagi sambungan ke rangkaian awam, atau rangkaian lain di luar premis menggunakan aset ICT pengguna; g) memastikan pengguna mematuhi kawalan capaian penggunaan aset ICT pengguna; h) memastikan pengguna menggunakan kata laluan bagi penyimpanan maklumat terperingkat JPA; i) memastikan aset ICT pengguna mempunyai perisian *antivirus*; j) memastikan peraturan berkaitan *remote disabling, deletion* atau *lockout* dipatuhi; k) memastikan pengguna melaksanakan sandaran bagi maklumat yang disimpan di dalam aset ICT; l) menggunakan perkhidmatan web dan aplikasi yang dibenarkan sahaja; m) memastikan pengasingan *(hard disk partition)* data dan perisian pada aset ICT pengguna; dan n) JPA berhak untuk mengambil tindakan yang sesuai seperti penamatan akses sekiranya didapati tidak mematuhi peraturan dalam polisi ini.	Pengguna

4.1.2 Tanggungjawab Pengguna	Tanggungjawab
Pengguna aset ICT JPA hendaklah mengambil kira perkara seperti yang berikut: a) *log out* perisian aplikasi apabila selesai tugas; b) mengaktifkan mekanisme pengunci atau kawalan yang bersesuaian seperti *password protected screen saver*; c) *log out* kerangka utama, *server* dan komputer pejabat apabila sesi bertugas selesai; dan d) melindungi aset ICT daripada kecurian atau kecuaian.	Pengguna

4.1.3 Penggunaan aset ICT Persendirian atau *Bring Your Own Device* (BYOD)	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) mengasingkan penggunaan bagi tujuan peribadi dan tugasan rasmi. Instalasi perisian yang dibekalkan oleh JPA pada aset ICT persendirian hendaklah mendapatkan kelulusan Pengurus ICT; b) membenarkan akses kepada maklumat yang berkaitan dengan tugasan rasmi dan menghapuskan data rahsia rasmi pada aset ICT persendirian apabila tidak digunakan lagi; c) memastikan hak harta intelek adalah di bawah tanggungjawab pengguna aset ICT persendirian; d) penyalahgunaan aset ICT persendirian adalah di bawah tanggungjawab pengguna sendiri; e) JPA tidak bertanggungjawab ke atas sebarang kerosakan sistem operasi atau perkakasan aset ICT persendirian; dan f) JPA menghormati privasi aset ICT persendirian dengan mengambil langkah pencegahan yang terbaik untuk memastikan keselamatan maklumat. JPA mempunyai hak untuk menjejaki dan meminta akses kepada aset ICT persendirian sekiranya terdapat pelanggaran keselamatan maklumat yang dikenal pasti.	Pengurus ICT Warga JPA

4.1.4 Sambungan Rangkaian Tanpa Wayar untuk aset ICT	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) mengkonfigurasi rangkaian tanpa wayar aset ICT untuk melindungi daripada protokol yang mempunyai kelemahan; b) menetapkan *bandwidth* rangkaian yang bersesuaian bergantung kepada jenis akses; dan c) tidak mendedahkan identiti dan kata laluan sambungan rangkaian tanpa wayar.	Pentadbir ICT JPA Pengguna

4.2 Kebenaran Hak Akses

Objektif

Memastikan akses pengguna, komponen perisian dan perkhidmatan yang disediakan hanya diberikan kepada pengguna yang dibenarkan.

4.2.1 Hak Capaian	Tanggungjawab
Prosedur penetapan dan penggunaan ke atas hak akses hendaklah mengambil kira perkara berikut: a) mengenal pasti pengguna yang memerlukan hak akses untuk sistem aplikasi, sistem pengoperasian dan pengurusan pangkalan data; b) penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat, atas prinsip perlu mengetahui (*need-to-know-basis*); c) keperluan capaian hendaklah sentiasa dipantau dan dikemas kini bagi memastikan hak capaian ini diberikan kepada pegawai dan kakitangan yang dibenarkan sahaja; d) memastikan pengguna mengetahui tanggungjawab hak akses yang diterima; e) memastikan perbezaan peranan akses untuk pentadbir dan pengguna; f) sekiranya berlaku perubahan struktur organisasi di JPA, penetapan dan penggunaan ke atas hak akses perlu disemak semula berdasarkan keperluan skop tugas; g) melarang penggunaan ID pentadbir seperti *root* bagi akses ke konfigurasi sistem; h) memberikan hak akses sementara untuk perubahan atau penyelenggaraan yang dilaksanakan oleh Pihak Luaran; i) merekodkan semua log masuk untuk kegunaan jejak audit; j) tidak berkongsi ID pengguna dengan orang lain; k) menggunakan ID pengguna berdasarkan skop tugas (melaksanakan tugasan harian) dan tidak menggunakan ID pentadbir; dan l) sebarang perubahan mestilah mendapat kebenaran secara bertulis dan direkodkan.	ICTSO Pentadbir ICT JPA Pengguna

4.3 Kawalan Akses Maklumat

Objektif

Memastikan hanya akses yang dibenarkan ke atas maklumat dan aset yang berkaitan.

4.3.1 Akses Maklumat dan Aset yang Berkaitan	Tanggungjawab
Bagi memastikan kawalan had akses ke atas maklumat dan aset yang berkaitan, perkara berikut hendaklah dipatuhi: a) tidak membenarkan akses ke maklumat terperingkat bagi pengguna yang tidak dibenarkan; b) menyediakan konfigurasi untuk mengawal akses maklumat di dalam sistem, aplikasi dan perkhidmatan; c) mengawal data yang boleh diakses mengikut kategori pengguna; d) mengawal individu dan kumpulan yang telah dikenal pasti mempunyai akses seperti *read, write, delete* dan *execute*; e) menyediakan kawalan fizikal atau kawalan hak akses untuk aplikasi data atau sistem; f) aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini; g) mengehadkan kemasukan kata laluan bagi capaian kepada aplikasi adalah maksimum tiga (3) kali sahaja. Setelah mencapai tahap maksimum, capaian akan disekat sehingga ID capaian diaktifkan semula; dan h) akses maklumat melalui capaian jarak jauh adalah tidak digalakkan, penggunaannya terhad kepada perkhidmatan yang diberi kebenaran sahaja.	ICTSO Pentadbir ICT JPA

4.3.2 Akses Maklumat Rahsia Rasmi	Tanggungjawab
Untuk melindungi maklumat rahsia rasmi yang kritikal kepada JPA, pengurusan akses perlu mematuhi perkara berikut: a) melaksanakan kawalan untuk akses maklumat mengikut tempoh masa yang dibenarkan; b) melaksanakan kawalan untuk akses maklumat yang diberikan kepada Pihak Luaran; c) memantau dan menguruskan semua penggunaan atau penyebaran maklumat secara *real-time*; d) maklumat hendaklah dilindungi daripada perubahan, penyalinan dan pengedaran yang tidak dibenarkan (termasuk percetakan); dan e) merekodkan sebarang perubahan ke atas maklumat tersebut.	ICTSO Pentadbir ICT JPA

4.3.3 Kawalan Pengurusan Akses Maklumat dan Aset yang Berkaitan	Tanggungjawab
Perkara yang perlu dilaksanakan untuk melindungi maklumat adalah: a) menetapkan kawalan kebenaran akses berdasarkan identiti, peranti, lokasi atau aplikasi; b) menetapkan klasifikasi maklumat yang perlu dilindungi; c) mewujudkan proses pemantauan dan pelaporan; d) mendapatkan pengesahan dan kebenaran untuk mengakses maklumat; e) mengehadkan akses seperti mempunyai had masa yang dibenarkan; f) menggunakan enkripsi untuk melindungi maklumat (jika perlu); g) menetapkan kebenaran untuk mencetak maklumat (jika perlu); dan h) menghantar pemakluman jika terdapat insiden penyalahgunaan maklumat.	ICTSO Pentadbir ICT JPA

4.4 Akses Kepada Kod Sumber

Objektif

Akses kepada kod sumber dan persekitaran pembangunan hendaklah dikawal. Ini adalah untuk mengelakkan perubahan yang tidak dibenarkan bagi mengekalkan kerahsiaan.

Kawalan Kod Sumber	Tanggungjawab
Perkara berikut perlu dipatuhi untuk mengawal akses kepada kod sumber bagi meminimumkan potensi kegagalan sistem aplikasi: a) menguruskan akses kepada kod sumber dan program; b) *source libraries* berdasarkan prosedur yang ditetapkan; c) membenarkan akses *read* dan *write* mengikut kebenaran dan menguruskan risiko penyalahgunaan kod sumber; d) pengemaskinian kod sumber serta pemberian akses kepada kod sumber perlu mematuhi prosedur kawalan perubahan yang diluluskan; e) tidak membenarkan pengaturcaraan sistem mempunyai akses secara terus kepada repositori kod sumber tetapi melalui perisian pembangunan yang mengawal aktiviti dan kebenaran kepada kod sumber; f) menyimpan senarai kod sumber di tempat selamat dan memberikan kawalan akses kepada individu yang dibenarkan; g) menyimpan log audit akses dan perubahan kepada kod sumber; dan	Pentadbir ICT JPA Pihak Luaran

h) memastikan kod sumber bagi sistem aplikasi atau perisian yang dibekalkan oleh Pihak Luaran ketiga menjadi hak milik JPA.

4.5 Pengesahan Selamat (*Secure Authentication*)

Objektif

Memastikan pengguna atau individu menggunakan pengesahan yang sah untuk akses kepada sistem aplikasi dan perkhidmatan yang disediakan.

Pengesahan Prosedur Log Masuk yang Selamat	**Tanggungjawab**
Bagi sistem yang kritikal, penggunaan *multi-factor authentication* adalah digalakkan. Prosedur log masuk perlu mematuhi perkara seperti yang berikut: a) memaparkan maklumat hanya selepas log masuk berjaya; b) memaparkan notis amaran sistem hanya boleh diakses oleh pengguna yang sah; c) tidak memaparkan mesej kesilapan semasa log masuk; d) mengesahkan maklumat identiti yang dikunci masuk (key-in) untuk log masuk mencukupi dan betul; e) melindungi ID pengguna dan kata laluan daripada cubaan log masuk *brute force*; f) merekodkan jejak audit log masuk yang berjaya dan gagal; g) menghantar notis keselamatan jika ada potensi percubaan atau pencerobohan ke atas log masuk yang dikesan; h) tidak memaparkan kata laluan semasa log masuk; i) tidak menghantar kata laluan dalam *clear text* melalui rangkaian; j) menamatkan sesi yang tidak aktif dalam tempoh masa yang ditetapkan; dan k) mengehadkan tempoh masa sambungan bagi sistem yang kritikal.	ICTSO Pentadbir ICT JPA

4.6 Pengurusan Kapasiti

Objektif

Memastikan penggunaan sumber, seperti tenaga, ruang penyimpanan, atau sumber manusia, akan dipantau dan diubah suai agar sesuai dengan keperluan kapasiti semasa dan keperluan pada masa hadapan.

4.6.1 Pengurusan Kapasiti	Tanggungjawab
Perkara seperti berikut perlu diambil kira:	ICTSO
a) kapasiti sistem ICT hendaklah dirancang, diurus dan dikawal dengan terperinci bagi memastikan keperluannya adalah mencukupi serta bersesuaian untuk pembangunan dan operasi sistem ICT semasa atau pada masa akan datang; b) keperluan kapasiti perlu mengambil kira ciri-ciri keselamatan bagi meminimumkan risiko gangguan kepada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang; c) pemantauan kapasiti sistem ICT perlu dilaksanakan untuk memastikan ketersediaan dan kecekapan sistem; d) pengujian tekanan (stress test) ke atas sistem dan perkhidmatan hendaklah dilaksanakan untuk memastikan kapasiti mencukupi terutamanya semasa waktu puncak; dan e) dokumen pengurusan kapasiti sumber perlu disediakan terutamanya untuk sistem kritikal.	Pentadbir ICT JPA

4.6.2 Peningkatan Kapasiti	Tanggungjawab
Perkara berikut perlu dipatuhi untuk meningkatkan kapasiti sumber:	ICTSO
a) memastikan sumber manusia mencukupi; b) menyediakan kemudahan dan ruang kerja yang kondusif; c) melaksanakan perolehan bagi kapasiti yang tidak mencukupi agar sesuai dengan keperluan semasa dan masa hadapan; dan d) menggunakan pengkomputeran awan (cloud computing) sekiranya perlu.	Pentadbir ICT JPA

4.6.3 Pengurangan Kapasiti	Tanggungjawab
Perkara berikut perlu dipatuhi untuk mengurangkan kapasiti sumber:	ICTSO
a) menghapuskan data lama (disk space) yang tidak digunakan lagi; b) melupuskan rekod fizikal mengikut jadual pelupusan rekod jabatan yang telah diluluskan; c) melupuskan sistem aplikasi, pangkalan data atau perkhidmatan ICT yang tidak digunakan lagi;	Pentadbir ICT JPA

d) mengoptimumkan proses *batch* dan *scheduler*;
e) mengoptimumkan kod aplikasi dan kuiri pangkalan data; dan
f) mengehadkan *bandwidth* bagi perkhidmatan ICT yang menggunakan kapasiti tinggi (jika perlu).

4.7 Perlindungan Terhadap Perisian Hasad (Malware)

Objektif

Memastikan perisian dan aset berkaitan ICT dilindungi daripada perisian hasad *(malware)*. Perlindungan terhadap perisian hasad hendaklah berdasarkan maklumat pengesanan dan pembaikan perisian hasad tersebut, kesedaran keselamatan, akses sistem yang sesuai serta kawalan pengurusan perubahan.

Perlindungan Daripada Perisian Hasad	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) melaksanakan kawalan untuk mencegah dan mengesan perisian yang tidak sah; b) melaksanakan kawalan untuk mencegah dan mengesan laman web yang tidak diketahui dan disyaki tidak selamat; c) mengurangkan kelemahan yang boleh dieksploitasi oleh perisian hasad (malware); d) melaksanakan pengesahan ke atas perisian dan maklumat sistem secara berkala terutamanya yang melibatkan sistem kritikal; e) mewujudkan langkah-langkah perlindungan terhadap risiko daripada fail dan perisian yang diperoleh sama ada melalui rangkaian luar atau pada mana-mana medium lain; f) memastikan perisian keselamatan yang digunakan sentiasa dikemas kini untuk mengimbas komputer dan media storan elektronik. Pengimbasan yang dilaksanakan merangkumi: i. mengimbas sebarang data yang diterima melalui rangkaian atau melalui sebarang bentuk media storan elektronik sebelum digunakan; ii. mengimbas e-mel dan lampiran yang dimuatturun sebelum digunakan; dan iii. mengimbas laman web yang diakses. g) menetapkan konfigurasi perisian keselamatan untuk mengesan ancaman risiko; i. menyediakan polisi berdasarkan amalan terbaik (best practise); dan ii. teknik untuk menyekat serangan perisian hasad.	ICTSO Pentadbir ICT JPA Pengguna

h) melindungi daripada serangan perisian hasad semasa proses penyelenggaraan;
i) memberi kebenaran secara sementara atau kekal untuk menutup perisian pengesanan serangan hasad sekiranya ianya mengganggu operasi harian dengan mendapatkan kelulusan dan direkodkan;
j) menyediakan proses pemulihan dari serangan *malware*, termasuklah data dan perisian *backup*;
k) mengasingkan persekitaran yang berisiko akan menghadapi bencana;
l) menyediakan prosedur kawalan serangan perisian hasad termasuk latihan, proses pemulihan dan pelaporan;
m) menyediakan program kesedaran atau latihan mengenai ancaman perisian berbahaya dan cara mengendalikannya;
n) melaksanakan pengumpulan maklumat perisian hasad yang terkini untuk langkah-langkah pencegahan;
o) mengesahkan maklumat yang berkaitan dengan serangan hasad daripada sumber yang sahih; dan
p) memasukkan klausa tanggungan dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya.

4.8 Pengurusan Teknikal Ke Atas Kerentanan

Objektif

Mendapatkan maklumat tentang kelemahan yang mungkin wujud dalam sistem maklumat yang digunakan seterusnya mencegah eksploitasi kerentanan teknikal dalam sistem tersebut.

4.8.1 Mengenal Pasti Kerentanan Teknikal	Tanggungjawab
Inventori aset hendaklah mengandungi maklumat sistem seperti nama sistem, perisian yang digunakan, nombor versi dan pemilik yang bertanggungjawab ke atas perisian tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) menetapkan peranan dan tanggungjawab untuk mengurus kelemahan teknikal seperti pemantauan kelemahan, penilaian risiko, pengemaskinian *patches* dan lain-lain; b) mengenal pasti sumber maklumat yang akan digunakan untuk mengesan kelemahan teknikal yang berkaitan dan sentiasa	ICTSO Pentadbir ICT JPA Penyelaras ICT Bahagian

mengemas kini senarai aset sekiranya ada perubahan teknologi atau perisian yang digunakan;

c) memastikan kandungan kontrak perjanjian dengan Pihak Luaran merangkumi pengurusan dan pelaporan penemuan kelemahan teknikal yang berkaitan;
d) menjalankan pengujian keselamatan untuk mengenal pasti kelemahan yang ada dan memastikan baik pulih dilaksanakan;
e) merancang, merekod dan menguji penilaian keselamatan secara berkala oleh Pentadbir ICT JPA atau Pihak Luaran yang berkelayakan; dan
f) memastikan penggunaan *libraries* dan kod sumber luar yang selamat.

4.8.2 Penilaian Kelemahan Teknikal	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) menyemak dan mengesahkan laporan pengujian penilaian keselamatan; dan b) mengenal pasti risiko dan mengambil tindakan pemulihan ke atas penemuan daripada pengujian keselamatan yang telah dilaksanakan.	Pentadbir ICT JPA Penyelaras ICT Bahagian

4.8.3 Panduan Menangani Kelemahan Teknikal	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) mengambil tindakan yang bersesuaian mengikut tempoh masa yang ditetapkan setelah kelemahan dikenal pasti; b) tindakan mengatasi kelemahan teknikal berdasarkan kategori risiko merujuk kepada pengurusan perubahan atau prosedur pengurusan pengendalian insiden keselamatan; c) menggunakan perisian yang terkini daripada sumber yang sah; d) menguji dan menilai pengemaskinian *patches* yang telah dilaksanakan sebelum dipasang pada persekitaran sebenar; e) memastikan *patches* sentiasa dikemas kini terutamanya kepada sistem kritikal di JPA; f) menguji keberkesanan ke atas tindakan pemulihan yang telah dilaksanakan; g) sekiranya pengemaskinian tidak berjaya dilaksanakan, kawalan berikut perlu dipatuhi: i. menggunakan cadangan lain yang diberikan oleh sumber yang sahih (sekiranya ada); ii. menutup perkhidmatan yang terdedah akibat daripada kelemahan teknikal;	ICTSO Pentadbir Sistem Aplikasi Pentadbir Rangkaian dan Keselamatan Pentadbir ICT JPA

iii. menambah polisi kawalan akses di segmen rangkaian untuk melindungi sistem, peranti atau aplikasi yang terdedah daripada serangan;
iv. meningkatkan pemantauan untuk mengesan serangan sebenar;
v. meningkatkan kesedaran berkaitan dengan kelemahan teknikal; dan

h) proses pengurusan kelemahan teknikal harus dipantau dan dinilai secara berkala.

4.9 Pengurusan Konfigurasi

Objektif

Memastikan konfigurasi perkakasan, perisian, perkhidmatan dan rangkaian ICT berfungsi dengan baik dan mengambil kira aspek keselamatan.

4.9.1 Pengurusan Penetapan Konfigurasi	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) memastikan konfigurasi semua perkhidmatan dan perkakasan ditetapkan mengikut keperluan; dan b) peranan, tanggungjawab dan prosedur perlu disediakan untuk memastikan kawalan ke atas perubahan konfigurasi.	ICTSO Pentadbir ICT JPA Penyelaras ICT Bahagian

4.9.2 Amalan Baik (Best Practise)	Tanggungjawab
Templat standard untuk konfigurasi perkakasan, perisian, perkhidmatan dan rangkaian perlu disediakan seperti yang berikut: a) menggunakan panduan umum atau amalan terbaik yang tersedia daripada templat Pihak Luaran atau jabatan lain; b) mempertimbangkan tahap perlindungan yang diperlukan untuk menentukan tahap keselamatan yang mencukupi; c) menyokong dasar keselamatan maklumat yang sedang berkuat kuasa; d) mempertimbangkan keupayaan dan kebolehgunaan konfigurasi keselamatan mengikut keperluan; e) penyeragaman masa (clock synchronization); f) menukar kata laluan asal selepas proses instalasi dan penyemakan parameter keselamatan; g) menyediakan *log off* secara automatik mengikut tempoh yang ditetapkan; h) mematuhi terma dan syarat penggunaan lesen; dan	ICTSO Pentadbir ICT JPA Penyelaras ICT Bahagian

i) memastikan salinan sandaran maklumat, perisian dan sistem diselenggara serta diuji secara berkala.

4.9.3 Pengurusan Sandaran	Tanggungjawab
Melaksanakan proses sandaran dan pemulihan sama ada maklumat di Pusat Data JPA, Pusat Pemulihan Bencana atau lokasi yang dibenarkan serta perlu memastikan perkara berikut dipatuhi: a) memastikan prosedur sandaran dan pemulihan direkodkan dengan lengkap; b) memastikan keperluan keselamatan maklumat bagi proses sandaran dan pemulihan dipenuhi ke atas sistem kritikal JPA yang telah dikenal pasti; c) memastikan salinan sandaran disimpan di lokasi dan jarak yang selamat untuk mengelakkan sebarang kerosakan akibat bencana di Pusat Data JPA; d) memastikan perlindungan yang sesuai diberikan ke atas maklumat sandaran selari dengan Pusat Data JPA; e) menguji sistem sandaran dan pemulihan bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; f) menetapkan tempoh simpanan maklumat sandaran yang disimpan dan maklumat tersebut perlu dihapus setelah melepasi tempoh yang ditetapkan; g) menyediakan prosedur pengurusan sandaran dan pemulihan; h) membuat aktiviti klon ke atas semua maklumat dan sistem perisian mengikut keperluan atau apabila berlaku perubahan versi; dan i) menyimpan salinan sandaran sekurang-kurangnya di dalam dua (2) media storan yang berasingan.	ICTSO Pentadbir ICT JPA

4.10 Penghapusan Maklumat

Objektif

Memastikan penghapusan maklumat dilaksanakan mematuhi keperluan undang-undang dan peraturan yang berkuat kuasa.

4.10.1 Penghapusan Maklumat	Tanggungjawab
Perkara berikut hendaklah dipatuhi semasa menghapus maklumat pada sistem, aplikasi dan perkhidmatan: a) memilih kaedah penghapusan yang sesuai; b) merekodkan keputusan penghapusan sebagai bukti;	ICTSO Pentadbir ICT JPA

c) bukti penghapusan maklumat perlu disediakan oleh pembekal sekiranya menggunakan perkhidmatan pembekal untuk penghapusan maklumat; dan d) memastikan klausa penghapusan maklumat dimasukkan dalam perjanjian bersama pembekal bagi memastikan penguatkuasaan semasa dan selepas penamatan perkhidmatan.	Penyelaras ICT Bahagian Pihak Luar

4.10.2 Kaedah Penghapusan Maklumat	**Tanggungjawab**
Kaedah penghapusan maklumat perlu dipatuhi berdasarkan peraturan dan perundangan yang berkaitan. Maklumat terperingkat perlu dihapuskan sekiranya tidak diperlukan lagi mengikut kaedah berikut: a) menghapuskan versi, salinan dan fail sementara yang tidak boleh digunakan lagi; b) menggunakan pembekal yang diluluskan dan diperakui untuk melaksanakan perkhidmatan pelupusan; c) menggunakan perisian yang diiktiraf untuk pelupusan maklumat; d) menggunakan mekanisme yang bersesuaian untuk melupuskan media storan; e) penyedia perkhidmatan pengkomputeran awan perlu melaksanakan penghapusan maklumat mengikut peraturan yang ditetapkan; dan f) semasa peralatan dipulangkan kepada pembekal, media storan perlu disanitasi dan data dihapuskan untuk mengelakkan maklumat terperingkat terdedah.	ICTSO Pentadbir ICT JPA Penyelaras ICT Bahagian

4.11 Penyembunyian Data (Data Masking)

Objektif

Memastikan paparan data sensitif dihadkan mengikut peraturan, keperluan organisasi dan perundangan yang berkuat kuasa.

4.11.1 Teknik Penyembunyian Data	**Tanggungjawab**
Antara teknik untuk penyembunyian data dalam sistem aplikasi termasuk: a) enkripsi (pengguna yang mempunyai *decryption key* sahaja boleh melihat data tersebut); b) menggantikan data dengan *"Null"* atau menghapuskan salah satu huruf/ nombor (menghalang pengguna yang tidak dibenarkan untuk melihat mesej penuh); c) mengubah nombor atau tarikh dari nilai sebenarnya;	Pentadbir ICT JPA

d) penggantian data (menukar satu nilai kepada yang lain untuk menyembunyikan data sensitif); dan
e) menukar nilai dengan nilai *hash (hash value)*.

4.11.2 Pelaksanaan Penyembunyian Data	Tanggungjawab
Semasa melaksanakan penyembunyian data, perkara berikut perlu dipatuhi: a) tidak semua data diberikan akses kepada pengguna. Sistem aplikasi hanya memaparkan data minimum kepada pengguna; b) keperluan perundangan atau peraturan yang berkuat kuasa hendaklah dipatuhi; c) menyediakan kawalan akses kepada data yang diproses; dan d) menyediakanjejak audit untuk merekodkan penyediaan dan penerimaan data yang diproses.	Pentadbir ICT JPA

4.12 Pencegahan Kebocoran Data (Data Leakage Prevention)

Objektif

Memastikan langkah-langkah pencegahan kebocoran data dilaksanakan pada sistem, rangkaian dan sebarang peranti lain yang memproses, menyimpan atau menghantar maklumat terperingkat.

4.12.1 Pelaksanaan Pencegahan Kebocoran Data	Tanggungjawab
Perkara yang perlu dilaksanakan adalah seperti yang berikut: a) mengenal pasti dan mengklasifikasikan maklumat untuk melindungi kebocoran maklumat; b) memantau punca atau saluran kebocoran data; c) melaksanakan langkah pencegahan untuk mengelakkan kebocoran data; d) mengehadkan capaian pengguna; dan e) memastikan proses sandaran maklumat dilindungi seperti penyulitan (encryption) dan kawalan akses.	Pentadbir ICT JPA

4.13 Sandaran Maklumat (Information Backup)

Objektif

Memastikan salinan sandaran maklumat, perisian dan sistem diselenggara serta diuji secara berkala.

Pengurusan Sandaran	Tanggungjawab
Melaksanakan proses sandaran dan pemulihan maklumat di Pusat Data JPA, Pusat Pemulihan Bencana atau lokasi yang dibenarkan serta perlu memastikan perkara berikut dipatuhi: a) memastikan prosedur sandaran dan pemulihan direkodkan dengan lengkap; b) memastikan keperluan keselamatan maklumat bagi proses sandaran dan pemulihan dipenuhi ke atas sistem kritikal JPA yang telah dikenal pasti; c) memastikan salinan sandaran disimpan di lokasi dan jarak yang selamat untuk mengelakkan sebarang kerosakan akibat bencana di Pusat Data JPA; d) memastikan perlindungan yang sesuai diberikan ke atas maklumat sandaran selari dengan Pusat Data JPA; e) menguji sistem sandaran dan pemulihan bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; f) menetapkan tempoh simpanan maklumat sandaran yang disimpan dan maklumat tersebut perlu dihapus setelah melepasi tempoh yang ditetapkan; g) menyediakan prosedur pengurusan sandaran dan pemulihan; h) membuat aktiviti klon ke atas semua maklumat dan sistem perisian mengikut keperluan atau apabila berlaku perubahan versi; dan i) menyimpan salinan sandaran sekurang-kurangnya di dalam dua (2) media storan yang berasingan.	ICTSO Pentadbir ICT JPA Pentadbir Sistem Aplikasi

4.14 *Redundancy* bagi Kemudahan Pemprosesan Maklumat

Objektif

Memastikan ketersediaan kemudahan operasi ICT.

Ketersediaan Kemudahan Pemprosesan Maklumat	Tanggungjawab
Mengenal pasti dan mereka bentuk arkitektur sistem dengan kemudahan *redundancy* yang bersesuaian. Perkara yang perlu dipatuhi adalah seperti berikut: a) menyediakan ketersediaan *redundancy* rangkaian bagi kemudahan operasi ICT; b) menyediakan lebih daripada satu (1) kemudahan pusat data yang berlainan lokasi; c) menggunakan sumber punca kuasa elektrik secara *redundancy*; d) menggunakan perkakasan atau perisian yang mempunyai fungsi *automatic load balancing*; dan e) mempunyai komponen pendua dalam perkakasan *server* atau rangkaian.	Pentadbir ICT JPA

4.15 Merekodkan Log *(Logging)*

Objektif

Memastikan log bagi aktiviti, pengecualian, kecacatan, dan peristiwa lain yang berkaitan harus dihasilkan, disimpan, dilindungi, dan dianalisis bagi menghalang daripada akses yang tidak dibenarkan.

4.15.1 Polisi Log Aktiviti	Tanggungjawab
Aktiviti log perlu mengandungi perkara seperti yang berikut:	ICTSO
a) ID pengguna; b) aktiviti sistem; c) tarikh, masa dan butiran aktiviti yang dilakukan; d) percubaan gagal dan berjaya akses masuk ke sistem; e) perubahan konfigurasi sistem; f) aktiviti sistem pengoperasian; dan g) menyimpan log audit untuk tempoh masa yang dipersetujui.	Pentadbir ICT JPA

4.15.2 Kawalan Perlindungan Log	Tanggungjawab
Semua pengguna yang mempunyai akses tidak dibenarkan memadam atau menyahaktifkan rekod log. Kawalan perlindungan ke	CDO

atas rekod log bertujuan untuk melindungi daripada perubahan yang tidak dibenarkan ke atas rekod log seperti yang berikut:

ICTSO

Pentadbir ICT JPA

a) merekodkan perubahan yang dilakukan;
b) fail log yang diubah atau dihapus;
c) Kegagalan merekodkan aktiviti log sekiranya media storan penuh;
d) melindungi maklumat log daripada capaian yang tidak dibenarkan;
e) capaian ke atas log fail *server* hanya kepada pengguna yang dibenarkan sahaja;
f) menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera;
g) sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir ICT JPA hendaklah melaporkan kepada ICTSO dan CDO;
h) merekodkan dan mengambil tindakan ke atas kesalahan, kesilapan dan/atau penyalahgunaan log; dan
i) memastikan masa (time stamp) dalam sistem aplikasi diselaraskan dengan waktu rekod log.

4.15.3 Analisis Log

Tanggungjawab

Rekod log perlu dianalisis untuk mengenal pasti aktiviti yang boleh menyebabkan sistem aplikasi dicerobohi oleh pihak yang tidak dibenarkan. Aktiviti analisis log perlu mengandungi perkara berikut:

ICTSO

CSIRT JPA

Pentadbir ICT JPA

a) melaksanakan analisis log;
b) merekodkan maklumat bagi setiap insiden atau kejadian keselamatan;
c) pengecualian yang dibenarkan telah dikenal pasti dalam polisi;
d) keputusan hasil analisis;
e) menyemak percubaan yang berjaya atau gagal kepada perkakasan rangkaian atau *server*; dan
f) memantau, menyemak dan menyelaras kesemua rekod log fizikal untuk mendapatkan analisis yang lebih tepat.

4.15.4 Log Pentadbir dan Pengguna	Tanggungjawab
Semua log aktiviti pentadbir dan pengguna sistem direkodkan dan log hendaklah dilindungi serta disemak secara berkala. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh sekurang-kurangnya satu tahun atau tempoh yang dipersetujui bagi membantu mengenal pasti kejadian insiden keselamatan; dan b) sekiranya wujud aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir ICT JPA hendaklah melaporkan kepada CSIRT JPA.	ICTSO CSIRT JPA Pentadbir ICT JPA

4.16 Aktiviti Pemantauan

Objektif

Memastikan rangkaian, sistem, dan aplikasi dipantau bagi sebarang aktiviti anomali yang meragukan supaya tindakan yang sesuai boleh diambil.

4.16.1 Aspek Pemantauan	Tanggungjawab
Tahap pemantauan ditetapkan mengikut keperluan keselamatan maklumat, dasar dan polisi undang-undang yang sedang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) trafik keluar masuk rangkaian dan sistem aplikasi; b) akses ke sistem, *server*, peranti rangkaian dan sebagainya; c) fail konfigurasi bagi aplikasi dan peralatan kritikal; d) log daripada peranti keselamatan; e) log aktiviti sistem aplikasi dan rangkaian; f) memastikan kod sumber yang sahih digunakan dan tidak diubah suai; dan g) penggunaan dan keupayaan sumber seperti CPU, *memory*, dan *bandwidth*.	ICTSO Pentadbir ICT JPA

4.16.2 Pemantauan Aktiviti Anomali	Tanggungjawab
Perkara yang perlu dipantau adalah seperti yang berikut: a) proses yang ditamatkan tanpa kebenaran; b) trafik aktiviti yang mengandungi perisian hasad atau meragukan daripada alamat domain atau *IP Address* yang telah dikenal pasti terjejas; c) ciri-ciri serangan yang dikenal pasti *seperti Distributed Denial-of-Services* (DDOS); d) aktiviti sistem yang luar biasa seperti *process injection*; e) proses yang melebihi kebiasaan dan menyebabkan kesesakan trafik; f) akses yang tidak dibenarkan ke atas sistem; g) pengimbasan tanpa kebenaran ke atas sistem dan rangkaian; h) cubaan akses sama ada berjaya atau tidak kepada kemudahan ICT yang dilindungi seperti *server* DNS; i) aktiviti pengguna atau sistem yang luar biasa daripada kebiasaan; dan j) serangan kod perosak (malicious code), halangan pemberian perkhidmatan (denial of service), spam, pemalsuan (forgery, phishing), pencerobohan (intrusion), ancaman (threats) dan kehilangan fizikal (physical loss).	ICTSO Pentadbir ICT JPA

14.16.3 Kawalan Pemantauan Aktiviti Anomali	Tanggungjawab
Perkara yang boleh dilaksanakan dalam pemantauan aktiviti anomali adalah seperti yang berikut: a) memanfaatkan atau menggunakan sistem *threat intelligence*; b) menggunakan kaedah senarai yang disekat atau dibenarkan; c) menggunakan penilaian teknikal keselamatan untuk mengenal pasti garis panduan ciri keselamatan yang dibenarkan; d) menggunakan sistem pemantauan keupayaan untuk mengesan trafik yang meragukan; dan e) menggunakan sistem log untuk tujuan pemantauan.	ICTSO Pentadbir ICT JPA

4.17 Penyelarasan Jam

Objektif

Memastikan semua aktiviti keselamatan serta data lain yang direkodkan selari dengan Waktu Piawai Malaysia (Malaysia Standard Time, MST).

Penyelarasan Waktu	Tanggungjawab
Perkara yang boleh dilaksanakan dalam penyelarasan waktu adalah seperti berikut: a) memastikan waktu bagi sistem pemprosesan maklumat atau peralatan hendaklah diselaraskan dengan Waktu Piawai Malaysia (MST); dan b) penyelarasan waktu bagi perkhidmatan awan hendaklah mengikut Penyedia Perkhidmatan Awan (Cloud Service Provider) dan perbezaannya perlu dipantau dan direkodkan untuk mengurangkan risiko percanggahan.	ICTSO Pentadbir ICT JPA Penyelaras ICT Bahagian

4.18 Penggunaan Program Utiliti Khas

Objektif

Memastikan penggunaan program utiliti tidak menjejaskan kawalan keselamatan maklumat bagi sistem aplikasi.

Penggunaan Program Utiliti Khas	Tanggungjawab
Panduan seperti di bawah perlu dipatuhi: a) mengehadkan dan mengawal bilangan pengguna yang dibenarkan untuk menggunakan program utiliti; b) memastikan penggunaan ID yang unik untuk pengesahan dan kebenaran akses; c) mengenal pasti dan mendokumentasikan program utiliti yang diberikan kebenaran; d) membenarkan penggunaan program utiliti pada waktu luar jangka (ad-hoc); e) menghapuskan dan menutup program utiliti yang tidak berkaitan; f) mengehadkan ketersediaan program utiliti; g) menyimpan log program utiliti; dan h) penggunaan program utiliti yang membebankan kapasiti (bandwidth) rangkaian perlu dihadkan.	ICTSO Pentadbir ICT JPA Pentadbir Pusat Data Pentadbir Rangkaian dan Keselamatan Pentadbir Pangkalan Data Pentadbir Aset ICT

4.19 Instalasi Perisian

Objektif

Memastikan penggunaan perisian yang dibenarkan pada peralatan ICT.

Pemasangan Perisian Pada Sistem Pengoperasian	Tanggungjawab
Perkara berikut perlu dipatuhi bagi sebarang pemasangan atau perubahan perisian: a) pengemaskinian versi sistem pengoperasian hanya boleh dilakukan oleh Pentadbir ICT JPA; b) memastikan hanya *"executable code"* yang diluluskan digunakan dalam sistem operasi; c) memasang dan mengemas kini perisian yang telah diuji keberkesanan sahaja; d) memastikan semua sumber *libraries* program yang terkini; e) menggunakan sistem pengurusan konfigurasi untuk mengawal konfigurasi dan dokumentasi sistem; f) menetapkan strategi pembentukan semula (rollback) sebelum perubahan dilaksanakan; g) memastikan log audit direkodkan bagi semua pengemaskinian; h) memastikan versi lama perisian diarkibkan dan direkodkan untuk kegunaan memproses data sekiranya diperlukan; i) hanya perisian yang dibenarkan bagi kegunaan di JPA; j) memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; dan k) mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.	ICTSO Pengurus ICT Pentadbir ICT JPA Pentadbir Sistem Aplikasi Pentadbir Aset ICT Pentadbir Pusat Data Pentadbir Pangkalan Data Pentadbir Rangkaian dan Keselamatan

4.20 Keselamatan Rangkaian

Objektif

Memastikan pengurusan keselamatan perkhidmatan rangkaian dilaksanakan bagi melindungi maklumat dan kemudahan ICT daripada ancaman.

Keselamatan Peranti Rangkaian	Tanggungjawab
Kawalan keselamatan ke atas rangkaian perlu dilaksanakan bagi melindungi daripada akses yang tidak dibenarkan.	ICTSO

Perkara yang perlu dipatuhi adalah seperti yang berikut:

Pentadbir Rangkaian dan Keselamatan

Pentadbir Bangunan

Warga JPA

a) tahap pengelasan maklumat yang diuruskan dalam rangkaian JPA;
b) menetapkan tanggungjawab dan prosedur bagi pengurusan peranti rangkaian;
c) memastikan pengemaskinian maklumat rangkaian secara berterusan seperti diagram rangkaian dan fail konfigurasi peranti;
d) mengasingkan tanggungjawab operasi rangkaian daripada operasi sistem ICT sekiranya perlu;
e) menetapkan kawalan untuk melindungi kerahsiaan dan integriti maklumat yang melalui rangkaian awam, rangkaian pihak ketiga atau rangkaian tanpa wayar;
f) memantau secara berkala log masuk untuk mengesan insiden keselamatan;
g) melaksanakan aktiviti pengurusan rangkaian secara berterusan bagi memastikan perkhidmatan yang optimum;
h) melaksanakan pengesahan pengguna sebelum mengakses rangkaian;
i) mengehadkan dan mengawal akses ke rangkaian;
j) memastikan kawalan dan mengehadkan ke atas semua peralatan lain yang akan menggunakan rangkaian JPA;
k) memastikan tindakan pengukuhan ke atas peranti rangkaian;
l) mengehadkan akses peranti rangkaian bagi Pentadbir Rangkaian dan Keselamatan berbanding pengguna biasa;
m) mengasingkan sementara segmen rangkaian yang terjejas sehingga dipulihkan semula;
n) menyahaktifkan protokol rangkaian yang terdedah kepada ancaman;
o) memastikan kawalan keselamatan yang sesuai untuk penggunaan *Virtual Private Network* (VPN);
p) peralatan rangkaian hendaklah diletakkan di lokasi yang bebas daripada risiko seperti banjir, gegaran dan habuk dengan merujuk Pentadbir Bangunan (JPA-BKP, INTAN-Pendaftar);
q) semua trafik rangkaian hendaklah melalui peranti keselamatan rangkaian JPA;
r) semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Aggrement* (SLA) yang telah ditetapkan;
s) penggunaan rangkaian tanpa wayar (*wireless*) LAN di JPA hendaklah mematuhi peraturan; dan
t) penggunaan perisian rangkaian seperti *network analyser* hendaklah mendapat kelulusan ICTSO.

4.21 Keselamatan Perkhidmatan Rangkaian

Objektif

Memastikan keperluan, mekanisme dan tahap keselamatan perkhidmatan rangkaian disemak, dilaksana dan dipantau.

4.21.1 Panduan Perkhidmatan Rangkaian	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) mempunyai kawalan akses kepada perkhidmatan rangkaian yang disediakan; b) melaksanakan pengesahan identiti bagi mengakses perkhidmatan rangkaian; c) mengawal akses kepada perkhidmatan rangkaian mengikut peranan yang diluluskan; d) menyediakan prosedur pengurusan rangkaian bagi kawalan keselamatan kepada perkhidmatan rangkaian; e) menggunakan kaedah yang selamat bagi mengakses perkhidmatan rangkaian seperti penggunaan *Virtual Private Network* (VPN) atau rangkaian tanpa wayar; f) merekodkan maklumat seperti masa, lokasi, dan lain-lain semasa penggunaan perkhidmatan rangkaian; g) memantau penggunaan perkhidmatan rangkaian; h) pengurusan perkhidmatan rangkaian hendaklah dikenal pasti dan dinyatakan dalam perjanjian perkhidmatan rangkaian; dan i) Pentadbir Rangkaian dan Keselamatan bertanggungjawab ke atas insiden keselamatan yang melibatkan perkhidmatan rangkaian.	ICTSO Pentadbir Rangkaian dan Keselamatan

4.21.2 Keselamatan Perkhidmatan Rangkaian	Tanggungjawab
Aspek keselamatan perkhidmatan rangkaian yang perlu mengambil kira seperti yang berikut: a) menggunakan teknologi keselamatan perkhidmatan rangkaian seperti pengesahan identiti, kawalan akses atau penggunaan enkripsi; b) memastikan peralatan rangkaian mematuhi polisi parameter yang ditetapkan bagi menjamin keselamatan sambungan rangkaian; c) memastikan kawalan akses kepada perkhidmatan rangkaian dan sistem aplikasi mengikut peranan yang diluluskan; d) memastikan trafik rangkaian dipantau dan dikawal oleh peralatan keselamatan; dan	ICTSO Pentadbir Rangkaian dan Keselamatan

e) menggunakan peralatan *Web Content Filtering* bagi mengawal akses ke laman web yang tidak dibenarkan.

4.22 Pengasingan Rangkaian

Objektif

Memastikan pengasingan kawalan sempadan ke atas perkhidmatan rangkaian yang disediakan untuk meminimumkan risiko ancaman atau pengubahsuaian yang tidak dibenarkan.

4.22.1 Panduan Pengasingan Rangkaian	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) menyediakan segmen yang hanya untuk kegunaan warga JPA; b) menetapkan segmen yang berbeza bagi pengguna biasa, pentadbir, pelayan, sistem aplikasi dan pihak ketiga; c) mengasingkan akses rangkaian mengikut tahap kritikal dan sensitiviti atau lain-lain keperluan; d) memastikan penggunaan peralatan keselamatan seperti *firewall* atau *router* bagi mengawal segmen rangkaian; *e)* melaksanakan polisi kawalan akses melalui *gateway* berdasarkan keperluan dan klasifikasi maklumat; f) mengasingkan rangkaian tanpa wayar dengan rangkaian dalaman kecuali dengan menggunakan kawalan keselamatan seperti *firewall*; g) mengasingkan akses rangkaian tanpa wayar untuk pelawat dan warga JPA; h) mengawal akses kepada peralatan rangkaian bagi pengguna yang dibenarkan sahaja; dan i) mengemas kini hak akses pengguna dan pentadbir sekiranya berlaku perubahan tanggungjawab.	ICTSO Pentadbir Rangkaian dan Keselamatan

4.23 Kawalan Penapisan Web

Objektif

Memastikan akses ke laman web dilindungi dan menyekat akses ke laman web yang tidak dibenarkan.

4.23.1 Panduan Penapisan Web	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) menyekat alamat IP atau domain laman web yang tidak sah; b) memantau laman web yang mempunyai fungsi muat naik maklumat; c) menyekat laman web berbahaya seperti *phishing* dan *malicious code*; d) mengemas kini pangkalan data (signature database) peralatan keselamatan web melalui sumber yang sahih; e) menyekat laman web perkongsian maklumat yang tidak sah *(illegal)*; f) memberikan latihan teknikal kepada kakitangan teknikal mengenai pengendalian peralatan laman web; dan g) memberikan program kesedaran kepada pengguna mengenai tatacara akses laman web yang selamat.	ICTSO Pentadbir Rangkaian dan Keselamatan

4.24 Penggunaan Kriptografi

Objektif

Memastikan penggunaan kriptografi untuk melindungi kerahsiaan dan integriti maklumat berdasarkan keperluan JPA dengan mematuhi keperluan undang-undang yang berkaitan.

4.24.1 Penggunaan Kriptografi	Tanggungjawab
Penggunaan kriptografi perlu mematuhi perkara seperti yang berikut: a) memaksimumkan faedah, meminimumkan risiko dan mengelak penyalahgunaan kriptografi berdasarkan kepada peraturan yang berkuat kuasa; b) mengenal pasti kriptografi yang hendak digunakan berdasarkan klasifikasi maklumat; c) memastikan perlindungan maklumat menggunakan kriptografi atau kaedah kawalan yang bersesuaian ke atas peranti mudah alih dan media storan yang dihantar menerusi rangkaian;	ICTSO Pentadbir ICT JPA Pentadbir Rangkaian dan Keselamatan Pentadbir Pusat Data Pentadbir Sistem Aplikasi

d) menetapkan peranan dan tanggungjawab bagi:
   i. pelaksanaan peraturan penggunaan kriptografi; dan
   ii. pengurusan kunci seperti penjanaan kunci.
e) menetapkan kesesuaian penggunaan kriptografi berdasarkan keperluan di JPA;
f) melaksanakan pemeriksaan ke atas kandungan maklumat sebelum dienkripsi bagi memastikan tiada *malware* dan kandungan berbahaya;
g) kandungan perjanjian perkhidmatan dengan pihak ketiga yang menyediakan perkhidmatan kriptografi perlu mengandungi tanggungjawab, kebolehpercayaan perkhidmatan dan masa tindak balas bagi penyediaan perkhidmatan;
h) maklumat perlu diklasifikasikan mengikut tahap peringkat maklumat seperti Rahsia Besar, Rahsia, Sulit dan Terbuka;
i) media storan seperti *external hard disk, thumb drive* dan sebagainya perlu dilaksanakan penetapan kata laluan bagi mengelakkan pencerobohan maklumat; dan
j) penggunaan *Secure Socket Layer* (SSL) adalah diwajibkan bagi semua sistem aplikasi atau pertukaran maklumat dengan pihak ketiga.

4.24.2 Pengurusan Kunci Kriptografi	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti yang berikut:	ICTSO
a) melaksanakan proses penjanaan, penyimpanan, mengarkibkan, pengambilan semula, pengagihan, penamatan dan pemusnahan kunci kriptografi;	Pentadbir ICT JPA
b) memastikan sistem pengurusan kunci kriptografi perlu berdasarkan piawaian, prosedur atau kaedah yang selamat;	Pentadbir Rangkaian dan Keselamatan
c) menjana kunci kriptografi yang berlainan bagi setiap sistem dan aplikasi;	Pentadbir Sistem Aplikasi
d) pengeluaran sijil kunci kriptografi umum;	
e) pengagihan kunci kriptografi kepada entiti berkaitan termasuk pengaktifan selepas penerimaan;	Pentadbir Pusat Data
f) penyimpanan dan cara akses kepada kunci kriptografi;	Pentadbir ICT JPA
g) penukaran atau pengemaskinian kunci;	
h) pengurusan kunci kriptografi yang terjejas;	
i) menyahaktifkan kunci kriptografi yang telah terjejas atau pengguna yang tamat perkhidmatan;	
j) menggantikan kunci kriptografi yang hilang atau rosak;	
k) mengarkib atau membuat pendua kunci kriptografi;	
l) memusnahkan kunci kriptografi;	
m) mengaudit atau merekodkan log aktiviti kunci kriptografi;	

n) menetapkan tempoh pengaktifan dan menyahaktifkan bagi kunci kriptografi;
o) memberikan kerjasama kepada pihak berkaitan sekiranya diperlukan;
p) kunci kriptografi perlu dilindungi daripada pengubahsuaian, kehilangan dan akses yang tidak dibenarkan; dan
q) peralatan atau perisian yang digunakan untuk menghasilkan, menyimpan, dan mengarkib kunci kriptografi perlu dilindungi.

4.24.3 Panduan Penggunaan Kriptografi Untuk Kawalan Keselamatan	Tanggungjawab
Penggunaan kriptografi disarankan berdasarkan kategori seperti yang berikut: a) kerahsiaan (confidentiality): menggunakan enkripsi untuk melindungi maklumat semasa penyimpanan atau penghantaran; b) integriti atau ketulenan (integrity or authenticity): menggunakan tandatangan digital untuk mengesahkan ketulenan atau integriti maklumat yang disimpan atau dihantar; c) tidak boleh disangkal (non-repudiation): menggunakan kriptografi ke atas bahan bukti bagi sesuatu peristiwa atau tindakan; dan d) pengesahan (authentication): menggunakan kriptografi untuk mengesahkan identiti pengguna atau transaksi yang melibatkan sistem aplikasi.	ICTSO Pentadbir ICT JPA Pentadbir Rangkaian dan Keselamatan Pentadbir Sistem Aplikasi Pentadbir Pusat Data Pentadbir ICT JPA

4.25 Kitaran Hayat Pembangunan Yang Selamat

Objektif

Memastikan pembangunan sistem aplikasi mengguna pakai kitar hayat pembangunan yang selamat

4.25.1 Panduan Pembangunan Sistem yang Selamat	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti berikut: a) aspek keselamatan pembangunan perlu diambil kira dalam perkhidmatan, infrastruktur, perisian dan sistem; b) mengasingkan persekitaran sebenar (production), pembangunan (development) dan (testing/staging);	ICTSO Pentadbir Rangkaian dan Keselamatan Pentadbir Sistem Aplikasi

c) menyediakan panduan keselamatan dalam kitar hayat pembangunan sistem *(development lifecycle)* yang mengambil kira: i. metodologi keselamatan pembangunan sistem; dan ii. garis panduan pengekodan selamat. d) keperluan keselamatan dalam fasa spesifikasi, reka bentuk dan pengurusan projek; e) pengujian keselamatan seperti ujian penembusan, semakan kod pengaturcaraan dan pengujian pepijat *(bugs)* kod pengaturcaraan selepas pengemaskinian; f) penyimpanan kod sumber dan konfigurasi sistem aplikasi di tempat yang selamat; g) memastikan kawalan keselamatan ke atas perubahan versi sistem aplikasi; h) menyediakan keperluan latihan keselamatan sistem aplikasi untuk meningkatkan kemahiran teknikal pengaturcaraan bagi mengenal pasti dan menyelesaikan kelemahan ke atas aplikasi; i) memastikan keperluan lesen diambil kira atau dan menggunakan alternatif lain bagi kawalan kos yang efektif; dan j) memastikan pembangunan yang dilaksanakan oleh pihak ketiga mengambil kira kitar hayat pembangunan secara selamat dalam dokumen kontrak/perjanjian.	Pentadbir Pusat Data

4.26 Keperluan Keselamatan Sistem Aplikasi

Objektif

Memastikan semua keperluan keselamatan maklumat dikenal pasti semasa pembangunan atau penambahbaikan sistem aplikasi.

4.26.1 Keperluan Keselamatan Aplikasi	Tanggungjawab
Keperluan keselamatan sistem aplikasi yang perlu diambil kira adalah seperti yang berikut: a) memastikan pengguna mempunyai tahap akses yang dibenarkan; b) mengenal pasti jenis maklumat dan tahap klasifikasi yang akan diproses oleh sistem aplikasi; c) membezakan had akses kepada data dan fungsi dalam sistem aplikasi;	ICTSO Pentadbir ICT JPA Pihak Ketiga

d) ketahanan terhadap ancaman perisian hasad atau gangguan pihak yang tidak dibenarkan;
e) memastikan perundangan dan peraturan dipatuhi bagi transaksi yang dijana, diproses, dilengkapkan atau disimpan;
f) menetapkan keperluan privasi bagi pihak yang terlibat;
g) memastikan maklumat rahsia rasmi dilindungi;
h) memastikan data yang diproses dan dipindahkan dilindungi;
i) memastikan komunikasi antara semua pihak dienkripsi dengan selamat;
j) melaksanakan pengesahan input;
k) mengawal kelulusan yang dijana oleh Sistem Aplikasi seperti mengehadkan kelulusan atau kelulusan melebihi satu orang pelulus;
l) mengawal kebenaran untuk akses kepada *output* yang dihasilkan;
m) mengehadkan kandungan medan *free text* bagi mengawal kapasiti storan;
n) melaksanakan pemantauan dan merekodkan log transaksi ke atas proses kerja;
o) memastikan kawalan keselamatan sistem aplikasi seperti penggunaan perisian log atau sistem pengesanan kebocoran data; dan
p) pengendalian mesej ralat.

4.26.2 Transaksi Perkhidmatan Dalam Talian	**Tanggungjawab**
Perkara-perkara berikut perlu dipatuhi: a) memastikan pengguna mempunyai tahap akses mengikut kelulusan atau kebenaran pemilik sistem; b) memastikan penggunaan mekanisme seperti *digital signature*, *hashing* dan lain-lain untuk mengesahkan identiti penghantar dan penerima semasa pertukaran data; c) memastikan pengesahan berkaitan dengan pihak yang berhak untuk meluluskan kandungan maklumat, penerbitan atau menandatangani dokumen transaksi; d) memastikan semua pihak memahami aspek kerahsiaan, integriti, serta bukti penghantaran dan penerimaan dokumen; e) memastikan perkhidmatan sistem aplikasi menggunakan *Secure Socket Layer* (SSL) dalam setiap transaksi; dan f) menetapkan tempoh transaksi yang disimpan.	ICTSO Pentadbir ICT JPA Pentadbir Sistem Aplikasi Pihak Ketiga

4.26.3 Aplikasi Pesanan dan Pembayaran Elektronik	Tanggungjawab
Perkara berikut perlu dipatuhi: a) mengekalkan kerahsiaan dan integriti maklumat pesanan atau pembayaran; b) mengesahkan maklumat pembayaran oleh pelanggan; c) mengelakkan kehilangan atau duplikasi maklumat transaksi; d) menyimpan maklumat transaksi di lokasi yang selamat dan tidak boleh diakses oleh orang ramai; dan e) menggunakan tandatangan atau sijil digital yang sah dan dikeluarkan oleh pihak yang diberi kuasa *(authority)*.	Pentadbir ICT JPA Pentadbir Sistem Aplikasi Pihak Ketiga

4.27 Prinsip Kejuruteraan dan Arkitektur Sistem yang Selamat (Secure System Architecture and Engineering Principles)

Objektif

Prinsip kejuruteraan keselamatan sistem hendaklah diwujudkan, didokumenkan, dikaji dan diguna pakai ke atas semua pembangunan sistem aplikasi.

4.27.1 Kriteria Kejuruteraan Sistem yang Selamat	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) menyediakan kawalan keselamatan yang diperlukan untuk melindungi maklumat dan sistem aplikasi daripada ancaman yang dikenal pasti; b) mempunyai keupayaan kawalan keselamatan untuk mencegah, mengesan atau melaksanakan tindakan ke atas insiden keselamatan; c) memastikan semua maklumat rahsia rasmi dienkripsi *(encryption)*; d) mengenal pasti keperluan kawalan keselamatan yang akan dilaksanakan; e) melaksanakan kawalan keselamatan terhadap individu yang berkaitan; f) memastikan prinsip kejuruteraan mengaplikasikan reka bentuk keselamatan *(security architecture)*; g) memastikan kawalan keselamatan infrastruktur seperti penggunaan *Public Key Infrastructure* (PKI), *Identity and Access Management* (IAM), pencegahan kebocoran data dan pengurusan akses dinamik;	Pentadbir ICT JPA Pentadbir Sistem Aplikasi Pihak Ketiga

h) mempunyai kepakaran untuk membangunkan dan menyelenggarakan sistem aplikasi selari dengan teknologi yang digunakan atau dipilih;
i) mengambil kira keperluan kos, masa dan cabaran dalam memenuhi keperluan keselamatan;
j) mengguna pakai konsep amalan terbaik *(best practise)*; dan
k) melaksanakan *Security Posture Assessment* (SPA) dan *hardening* ke atas sistem aplikasi.

4.27.2 Prinsip *"Zero Trust"*	**Tanggungjawab**
Perkara yang perlu diambil kira adalah seperti yang berikut: a) kawalan keselamatan tidak boleh bergantung sepenuhnya kepada peralatan keselamatan rangkaian; b) menyemak dan mengesahkan identiti bagi semua akses ke sistem aplikasi; c) memastikan sistem aplikasi menggunakan fungsi enkripsi; d) menyemak dan mengesahkan semua permohonan akses yang diterima; e) memberikan kategori akses paling minimum kepada pengguna; dan f) menggunakan pengesahan keselamatan ketika log masuk atau transaksi yang melibatkan sistem aplikasi seperti *captcha, security phrase* dan *Secure Transaction Authorisation Code* (TAC).	ICTSO Pentadbir ICT JPA Pentadbir Sistem Aplikasi Pihak Ketiga

4.28 Pengekodan Selamat

Objektif

Memastikan penggunaan kod pengaturcaraan yang selamat bagi meminimumkan kelemahan (vulnerabilities) dalam sistem aplikasi.

4.28.1 Fasa Perancangan Pengekodan Selamat	**Tanggungjawab**
Perkara yang perlu diambil kira adalah seperti yang berikut: a) pembangunan sistem aplikasi sama ada secara dalaman *(in-house)* atau luaran *(outsource)* hendaklah menggunakan pengekodan selamat berdasarkan kepada peraturan dan keperluan yang dikuat kuasakan; b) memastikan amalan dan kelemahan pengekodan yang berlaku sebelum ini dijadikan sebagai sumber rujukan supaya kelemahan keselamatan maklumat yang sama tidak berulang;	ICTSO Pentadbir ICT JPA Pentadbir Sistem Aplikasi Pihak Ketiga

c) menggunakan perisian Pembangunan seperti *Integrated Development Environments* (IDE) untuk membantu pengekodan selamat;
d) penggunaan persekitaran pembangunan semasa fasa pembangunan sistem aplikasi;
e) memastikan penggunaan perisian pembangunan yang terkini;
f) memastikan pengaturcaraan atau pihak ketiga yang dilantik mempunyai kemahiran dalam pembangunan sistem aplikasi menggunakan pengekodan selamat; dan
g) memastikan arkitektur, reka bentuk dan standard pengekodan digunakan dalam persekitaran yang selamat.

4.28.2 Fasa Semasa Pengekodan Selamat	**Tanggungjawab**
Perkara yang perlu diambil kira adalah seperti yang berikut: a) memastikan penggunaan teknik dan struktur pengekodan selamat bagi bahasa pengaturcaraan yang digunakan seperti *pair programming, refactoring* dan *test-driven development*; b) merekodkan dan memperbetulkan kelemahan kod sumber yang boleh terdedah kepada ancaman daripada dieksploitasi; c) menggunakan perisian yang terkini dan tidak tamat tempoh *End of Support* (EOS); d) memastikan tidak menggunakan Teknik Pembangunan yang tidak selamat seperti *hard-coded passwords, unapproved code samples* dan *unauthenticated web services*; e) melaksanakan pengujian keselamatan maklumat dan tindakan pembaikan; f) memastikan keupayaan integrasi dengan sistem maklumat yang lain; g) sebelum sistem aplikasi digunakan, perkara seperti di bawah hendaklah dilaksanakan: i. memastikan hak akses minimum pengguna; ii. melaksanakan analisis berkaitan kesalahan umum kod pengaturcaraan; dan iii. merekodkan tindakan pembetulan.	ICTSO Pentadbir ICT JPA Pentadbir Sistem Aplikasi Pihak Ketiga

4.28.3 Fasa Penyelenggaraan dan Kajian Semula	**Tanggungjawab**
Perkara yang perlu diambil kira adalah seperti yang berikut: a) memastikan *patches* dan *security updates* perisian sentiasa dikemas kini; b) kelemahan keselamatan maklumat yang dilaporkan hendaklah diambil tindakan;	ICTSO Pentadbir ICT JPA Pentadbir Sistem Aplikasi

c) ralat dan cubaan serangan hendaklah direkodkan serta disemak secara berkala bagi penambahbaikan ke atas kod pengaturcaraan sekiranya perlu; dan — Pihak Ketiga
d) kod sumber hendaklah dilindungi daripada akses dan gangguan yang tidak dibenarkan seperti menggunakan fungsi kawalan versi (version control).

Sekiranya menggunakan *libraries* luaran, perkara seperti di bawah hendaklah dilaksanakan:

a) memastikan *libraries* luaran yang digunakan adalah versi terkini;
b) menggunakan komponen seperti pengesahan kriptografi yang telah disahkan dan stabil;
c) memastikan lesen, keselamatan dan komponen luaran yang sah;
d) memastikan *libraries* boleh diselenggarakan dan diperoleh daripada sumber yang dipercayai; dan
e) ketersediaan sumber yang mencukupi untuk rujukan pembangunan jangka panjang.

Sekiranya *software package* perlu ditambah baik, perkara seperti di bawah hendaklah dipastikan:

a) risiko kepada fungsi kawalan sedia ada dan integriti perisian tersebut;
b) perlu mendapatkan kebenaran persetujuan daripada pihak ketiga;
c) keperluan untuk mendapatkan perubahan versi terkini;
d) iImplikasi yang akan berlaku sekiranya tanggungjawab penyelenggaraan diberikan kepada JPA; dan
e) keserasian (compatibility) dengan perisian yang lain.

4.29 Pengujian Keselamatan Semasa Pembangunan dan Penerimaan

Objektif

Memastikan keperluan keselamatan maklumat dipenuhi semasa sistem aplikasi diguna pakai dalam persekitaran sebenar.

4.29.1 Pengujian Keselamatan Sistem Aplikasi	Tanggungjawab
Pengujian keselamatan hendaklah merangkumi perkara berikut:	ICTSO
a) fungsi keselamatan sistem aplikasi hendaklah diuji semasa fasa pembangunan seperti pengesahan pengguna, kawalan akses, penggunaan kriptografi dan pengekodan selamat;	Pentadbir ICT JPA

b) konfigurasi keselamatan yang melibatkan sistem pengoperasian, *firewall*s dan komponen keselamatan lain hendaklah diuji;
c) *Security Posture Assessment* (SPA) hendaklah dilaksanakan ke atas semua sistem aplikasi baharu atau penambahbaikan sistem aplikasi;
d) menyemak dan mengesahkan data sebelum dikunci masuk dalam sistem aplikasi bagi menjamin ketepatan maklumat; dan
e) melaksanakan semakan dan pengesahan ke atas *output* data yang dihasilkan oleh sistem aplikasi.

Pentadbir Sistem Aplikasi

Pihak Ketiga

4.29.2 Pelan Pengujian Penerimaan Sistem

Tanggungjawab

Perkara yang perlu dipatuhi adalah seperti yang berikut:

a) menyediakan jadual aktiviti pengujian;
b) menyediakan *input* dan *output* yang dijangka supaya memenuhi senarai syarat yang telah ditentukan;
c) menetapkan kriteria untuk menilai keputusan;
d) memastikan proses kerja sistem aplikasi memenuhi keperluan pengguna;
e) melaksanakan pengujian fungsi ke atas sistem aplikasi menggunakan data palsu (dummy input);
f) melaksanakan keputusan pengujian yang memerlukan tindakan lanjut sekiranya diperlukan;
g) melaksanakan integrasi dan pengujian dengan sistem aplikasi yang lain sekiranya berkaitan; dan
h) melaksanakan ujian prestasi (performance test) dan ujian tekanan (stress test).

ICTSO

Pentadbir ICT JPA

Pentadbir Sistem Aplikasi

Pihak Ketiga

4.29.3 Pengujian Bebas bagi Pembangunan Dalaman dan Luaran

Tanggungjawab

Pengujian perlu dilaksanakan oleh selain daripada pasukan pembangunan sistem aplikasi. Perkara berikut perlu diambil kira seperti:

a) melaksanakan aktiviti semakan kod pengaturcaraan untuk mengenal pasti kelemahan termasuk *input* dan ralat yang tidak dijangka;
b) melaksanakan pengimbasan kelemahan untuk mengenal pasti konfigurasi yang tidak selamat dan kelemahan sistem aplikasi;
c) melaksanakan pengujian penembusan (penetration testing) untuk mengenal pasti reka bentuk dan kod sumber tidak selamat;
d) penilaian produk dan perkhidmatan hendaklah dilaksanakan sebelum perolehan dilaksanakan;
e) perjanjian bersama pihak ketiga perlu mengandungi keperluan keselamatan;

ICTSO

Pentadbir ICT JPA

Pentadbir Sistem Aplikasi

Pihak Ketiga

f) pembangunan secara luaran (outsource) atau pembelian komponen hendaklah mengikut tatacara perolehan; dan
g) persekitaran pengujian hendaklah sama dengan persekitaran sebenar supaya pengujian tersebut tidak boleh disangkal dan boleh dipercayai.

4.30 Pembangunan Sistem Secara Luaran

Objektif

Pembangunan sistem aplikasi yang dilaksanakan oleh pihak ketiga perlu dikawal selia dan dipantau bagi memastikan keselamatan maklumat dipatuhi.

Pembangunan Sistem Secara Luaran	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti yang berikut:	ICTSO
a) memastikan perjanjian lesen, *Intellectual Property Rights* (IPR) dan kod sumber menjadi hak milik kerajaan; b) memastikan spesifikasi perolehan mengandungi klausa berhubung keperluan keselamatan reka bentuk, keselamatan pengaturcaraan, pengujian, pensijilan keselamatan produk, ketersediaan kod sumber, keperluan pelupusan data, keutamaan terhadap teknologi dan kepakaran tempatan serta keperluan kompetensi pasukan pembangunan; c) menyediakan penilaian keselamatan oleh pihak ketiga; d) melaksanakan pengujian penerimaan untuk memastikan kualiti dan *output* memenuhi keperluan; e) memastikan pembuktian risiko penilaian keselamatan dan privasi di tahap minimum yang boleh diterima; f) memastikan pengujian keselamatan, kelemahan yang dikenal pasti dan tindakan pembetulan dilaksanakan adalah mencukupi sebelum penyerahan projek; g) menguatkuasakan bon perjanjian sekiranya pihak ketiga tidak memenuhi perkhidmatan; h) memasukkan klausa dalam kontrak yang membenarkan pelaksanaan audit terhadap proses pembangunan dan kod sumber; i) melaksanakan keperluan keselamatan untuk persekitaran pembangunan; j) mengambil kira perundangan yang berkuat kuasa seperti *Personal Data Act*; dan	Pentadbir ICT JPA Pentadbir Sistem Aplikasi Pihak Ketiga

k) sistem aplikasi perlu diangkat untuk kelulusan JPICT sebelum dibangunkan.

4.31 Pengasingan Persekitaran Pembangunan, Pengujian dan Sebenar

Objektif

Memastikan keselamatan maklumat dalam semua persekitaran ICT dilindungi daripada ancaman oleh pihak tidak dibenarkan.

4.31.1 Aspek Pengasingan Persekitaran ICT	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut:	ICTSO
a) mewujudkan prosedur keperluan sumber bagi penyediaan persekitaran untuk pembangunan, pengujian dan sebenar; b) mengasingkan persekitaran sebenar dengan pembangunan dalam domain yang berbeza secara *virtual* atau fizikal; c) menetapkan, merekodkan dan melaksanakan peraturan serta pengesahan untuk migrasi sistem aplikasi atau perisian daripada persekitaran pembangunan kepada persekitaran sebenar; d) melaksanakan pengujian ke atas perubahan sistem aplikasi di persekitaran pengujian sebelum digunakan dalam persekitaran sebenar; e) tidak menggunakan maklumat sebenar pada persekitaran pembangunan atau persekitaran pengujian kecuali dengan kawalan keselamatan; f) memastikan *compilers*, editor dan *tools* pembangunan atau program utiliti lain tidak boleh diakses daripada persekitaran sebenar apabila tidak diperlukan lagi; g) merekodkan semua penggunaan sumber yang dilaksanakan; dan h) memantau pelaksanaan penggunaan sumber bagi tujuan perancangan kapasiti.	Pentadbir ICT JPA Pentadbir Sistem Aplikasi Pentadbir Pusat Data Pentadbir Rangkaian dan Keselamatan Pihak Ketiga

4.31.2 Langkah Keselamatan bagi Persekitaran Pembangunan Pengujian dan Sebenar	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut:	ICTSO
a) mengemas kini *patches*, pembangunan sistem aplikasi, integrasi dan *tools* pengujian seperti *builders, integrators*, *compilers*, sistem konfigurasi dan *libraries*; b) memastikan keselamatan konfigurasi sistem aplikasi dan operasi perisian yang selamat;	Pentadbir Sistem Aplikasi

c) memantau dan memastikan kawalan akses persekitaran; d) memantau kawalan perubahan persekitaran dan kod yang disimpan; dan e) menyediakan sandaran *(backup)* persekitaran sebenar secara berkala.	Pentadbir Rangkaian dan Keselamatan Pentadbir Pusat Data

4.32 Pengurusan Perubahan

Objektif

Memastikan pengurusan perubahan dalam persekitaran ICT dilaksanakan dengan mengambil kira kawalan keselamatan maklumat.

4.32.1 Prosedur Kawalan Perubahan	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) merancang dan menilai impak yang mungkin berlaku ke atas pihak lain yang mempunyai kepentingan atau kebergantungan; b) memastikan perubahan yang dilaksanakan telah mendapat kelulusan; c) memastikan perubahan yang dilaksanakan dimaklumkan kepada pihak berkepentingan; d) perubahan atau pengubahsuaian ke atas perkakasan, perisian atau sistem aplikasi hendaklah diuji, direkodkan dan disahkan sebelum diguna pakai; e) memastikan pelaksanaan perubahan mengambil kira perancangan pembangunan; f) memastikan prosedur pembentukan semula (fallback) dilaksanakan sebagai pelan perancangan luar jangka (contingency); g) merekodkan semua perubahan yang dilaksanakan; h) memastikan manual operasi pengguna dan sistem aplikasi diubah mengikut keperluan; i) memastikan prosedur pelan kesinambungan perkhidmatan dan pemulihan ICT diubah mengikut keperluan; j) semua aspek mengawal pelaksanaan perubahan menggunakan prosedur kawalan perubahan; k) setiap perubahan kepada sistem pengoperasian perlu dikaji semula dan diuji untuk memastikan tiada sebarang masalah yang timbul terhadap keselamatan maklumat; l) perubahan kepada kod pengaturcaraan (source code) perlu dihadkan kepada Pentadbir Sistem Aplikasi yang dibenarkan; dan	ICTSO Pengurus ICT Pentadbir ICT JPA Pentadbir Sistem Aplikasi Pentadbir Rangkaian dan Keselamatan Pentadbir Pusat Data

m) memastikan aktiviti seperti memasang, menyenggara, menghapus dan mengemas kini mana-mana komponen ICT hendaklah mendapatkan kelulusan.

4.32.2 Kawalan Perubahan Kepada Platform	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) perubahan platform hendaklah dikaji bagi membolehkan pengujian yang bersesuaian dilakukan sebelum pelaksanaan; b) memastikan sistem aplikasi, integriti data dan kawalan akses disemak supaya operasi sistem tidak terjejas apabila perubahan platform dilaksanakan; c) ujian penerimaan pengguna perlu dilaksanakan setelah perubahan platform selesai dilaksanakan; dan d) memastikan perubahan yang sesuai diselaraskan kepada pelan kesinambungan perkhidmatan.	ICTSO Pentadbir Sistem Aplikasi Pentadbir Rangkaian dan Keselamatan Pentadbir Pusat Data Pentadbir ICT JPA

4.32.3 Kawalan Perubahan Kepada Perisian	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) memastikan perubahan pakej perisian mengambil kira aspek keselamatan maklumat; b) perubahan pakej perisian hanya dilaksanakan oleh pihak yang dibenarkan sahaja; c) melaksanakan pengujian ke atas pakej perisian yang terkini sebelum dimaklumkan kepada semua pengguna; dan d) memastikan perubahan pakej perisian tidak menjejaskan perkhidmatan operasi sistem maklumat.	Pentadbir ICT JPA

4.33 Data Pengujian

Objektif

Memastikan pemilihan data yang digunakan semasa pengujian dilindungi dan dikawal mengikut peraturan yang ditetapkan.

Panduan Penggunaan Data	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) melaksanakan kawalan akses yang sama di persekitaran sebenar dan persekitaran pengujian;	ICTSO Pentadbir Sistem Aplikasi

b) menyediakan hak akses berlainan setiap kali maklumat digunakan ke persekitaran pengujian; c) menyimpan log penyalinan dan penggunaan maklumat operasi bagi tujuan jejak audit; d) data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; e) data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat; f) melindungi maklumat terperingkat dengan pelaksanaan penyembunyian data dan menghapus data setelah pengujian selesai; dan g) menghapuskan maklumat operasi setelah pengujian selesai untuk mengelakkan data digunakan oleh pihak tidak dibenarkan.	Pentadbir Pusat Data Pentadbir Pangkalan Data

4.34 Perlindungan Sistem Maklumat Semasa Ujian Audit

Objektif

Memastikan penilaian pengujian audit dilaksanakan ke atas proses kerja sistem aplikasi.

Panduan Ujian Audit	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) mendapatkan kebenaran untuk capaian kepada sistem aplikasi dan data bagi ujian audit; b) mendapatkan kebenaran untuk melaksanakan ujian audit berdasarkan kawalan dan skop yang dibenarkan; c) memastikan data yang dibenarkan hanya berstatus *read only* semasa ujian audit dilaksanakan; d) jika terdapat keperluan capaian kepada sistem aplikasi, pengujian hendaklah dilaksanakan oleh pentadbir yang dibenarkan bagi membantu juruaudit; e) memastikan keperluan keselamatan perkakasan juruaudit dipatuhi seperti penggunaan antivirus sebelum kebenaran diberikan; f) membenarkan capaian kepada sistem fail oleh juruaudit dan menghapuskan data tersebut setelah audit selesai atau melaksanakan kawalan keselamatan yang bersesuaian; g) memastikan penggunaan peralatan audit (audit tools) mendapat kelulusan terlebih dahulu; h) melaksanakan ujian audit di luar waktu bekerja sekiranya menyebabkan gangguan perkhidmatan; dan i) menyimpan dan memantau semua akses semasa ujian audit.	ICTSO Pentadbir Sistem Aplikasi Pentadbir ICT JPA

GLOSARI

GLOSARI

BIL.	ISTILAH	PENERANGAN
1.	*Active Directory* (AD)	Teknologi *Microsoft* yang digunakan untuk mengurus komputer dan peralatan lain dalam rangkaian.
2.	Anomali	Keadaan atau sesuatu yang tidak biasa, luar biasa, atau menyimpang dari norma atau corak yang dijangkakan. Dalam konteks teknikal dan keselamatan maklumat, anomali sering digunakan untuk merujuk kepada tingkah laku atau kejadian yang berbeza daripada kebiasaan, yang mungkin menunjukkan terdapatnya masalah, kecacatan, atau ancaman
3.	Antivirus	Perisian yang mengimbas virus pada media storan, seperti cakera keras (*hard disk*) dan disket (diskette) untuk sebarang kemungkinan adanya virus.
4.	Aplikasi	Perisian komputer atau program yang khusus digunakan untuk peranti mudah alih.
5.	Aset Alih	Aset atau peralatan yang boleh dipindahkan atau dialihkan dari satu tempat ke tempat lain secara mudah termasuk Aset Alih yang dibekalkan bersekali dengan penyediaan bangunan atau infrastruktur lain.
6.	Aset ICT	Sesuatu yang bernilai yang boleh menyebabkan kerugian sekiranya berlaku kehilangan, kerosakan atau perubahan. Dalam konteks keselamatan maklumat, aset boleh dikategorikan kepada beberapa kumpulan antaranya proses kerja, data / maklumat, perisian, perkakasan, perkhidmatan, sumber manusia dan tapak / premis. (Surat Pekeliling Am Bilangan 3 Tahun 2024) Data, maklumat, perkakasan, perisian, aplikasi, dokumentasi dan sumber manusia serta premis berkaitan dengan ICT yang di bawah tanggungjawab JPA.
7.	*Backup*	Proses penduaan sesuatu dokumen atau maklumat.
8.	*Bandwidth*	Jalur lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh: di antara cakera keras dan PC utama) dalam jangka masa yang ditetapkan.
9.	Bilik khas	Bilik yang selamat dan terkawal.

BIL.	ISTILAH	PENERANGAN
10.	*Brute Force*	Teknik yang digunakan oleh pencuri atau penggodam untuk meneka kata laluan atau kunci kriptografi dengan mencuba semua kemungkinan kombinasi secara sistematik hingga berjaya.
11.	BYOD	*Bring Your Own Device*
12.	Capaian Jarak jauh	Capaian jarak jauh yang dimaksudkan merangkumi: i. capaian kepada sistem rangkaian dalaman; dan ii. capaian daripada sistem rangkaian luaran bagi lokasi luar pejabat untuk tujuan teleworking; atau iii. capaian Jarak Jauh merujuk kepada kemampuan untuk mengakses sistem komputer, rangkaian, atau sumber maklumat dari lokasi yang jauh atau bukan lokasi fizikal yang sama dengan sistem tersebut. Ini membolehkan pengguna untuk bekerja, mendapatkan maklumat, dan menjalankan tugas secara efektif tanpa perlu berada di lokasi yang sama dengan sumber yang ingin diakses.
13.	*CCTV*	*Closed-circuit television* Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
14.	CDO	*Chief Digital Officer* Ketua Pegawai Digital yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
15.	*Clear Desk* dan *Clear Screen*	Tidak meninggalkan dokumen data dan maklumat terperingkat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.
16.	CSIRT JPA	*Cyber Security Incident Response Team* Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan siber di agensi masing-masing dan agensi di bawah kawalannya.
17.	Penyembunyian Data	Penyembunyian Data (*Data masking*) merujuk kepada proses pengubahan data asli ke dalam bentuk yang tidak dapat dikenali atau tidak sensitif, sambil masih mengekalkan struktur dan format data tersebut. Tujuan utama data masking adalah untuk melindungi maklumat peribadi dan sensitif daripada akses tidak

BIL.	ISTILAH	PENERANGAN
		dibenarkan, terutamanya dalam situasi seperti pengujian sistem, analisis data, atau perkongsian data.
18.	*Denial of service*	Halangan pemberian perkhidmatan.
19.	DRC	*Disaster Recovery Centre* Pusat Pemulihan Bencana
20.	DRP	*Disaster Recovery Plan* Pelan Pemulihan Bencana
21.	EOS	*End of Support* Tamat Sokongan
22.	*Encryption*	Proses enkripsi (penyulitan) data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
23.	Fasiliti Perkhidmatan Sokongan	Merangkumi peralatan, kemudahan tempat, perkhidmatan penyelenggaraan, sistem notifikasi amaran dan pengujian berkala bagi memastikan kesinambungan perkhidmatan ICT.
24.	*Firewall*	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk peralatan atau perisian atau kombinasi kedua-duanya.
25.	*Forgery*	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).
26.	*Hard disk*	Cakera keras yang digunakan untuk menyimpan data dan boleh di akses lebih pantas.
27.	IAM	*Identity and Access Management*
28.	ICT	*Information and Communication Technology*
29.	ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
30.	IDE	*Integrated Development Environments*
31.	Insiden Keselamatan	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
32.	INTAN	Institut Tadbiran Awam Negara

BIL.	ISTILAH	PENERANGAN
33.	Internet	Sistem rangkaian seluruh dunia, di mana pengguna pada mana-mana komputer boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
34.	Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.
35.	IPR	*Intellectual Property Rights*
36.	ISMS	*Information Security Management System*
37.	JPICT	Jawatankuasa Pemandu ICT JPA
38.	JTICT	Jawatankuasa Teknikal ICT
39.	Klon	Merujuk kepada salinan yang tepat dan lengkap dari sistem, perisian, atau peranti, termasuk semua data dan konfigurasi yang ada. Klon biasanya digunakan untuk membuat usaha pemulihan yang lebih mendalam atau untuk membina persekitaran kerja yang identik.
40.	Kriptografi	Kaedah untuk menukar data dan maklumat biasa (piawaian format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
41.	LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
42.	*Log out*	Keluar daripada sesuatu sistem atau aplikasi komputer.
43.	*Malicious code*	Merujuk kepada sebarang kod, skrip, atau perintah yang direka untuk melakukan tindakan berbahaya, yang mungkin termasuk *malware*.
44.	NACSA	*National Cyber Security Agency* Agensi Keselamatan Siber Negara
45.	*Outsource*	Maklumat yang diproses dan diperoleh di luar daripada sesuatu organisasi atau struktur kerja.
46.	Pegawai Pengelas	Bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan dari segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa.
47.	Pegawai Keselamatan	Memastikan keselamatan perlindungan di jabatan terjamin sepanjang masa.

BIL.	ISTILAH	PENERANGAN
48.	Pegawai Rekod Jabatan	Memastikan pelabelan maklumat dilaksanakan bagi memudahkan pengurusan penyimpanan maklumat.
49.	Pembangun Sistem	Individu atau kumpulan teknikal atau Pihak Luaran yang bertanggungjawab dalam membangunkan sistem aplikasi berdasarkan spesifikasi keperluan sistem yang ditetapkan oleh pemohon/ pemilik proses.
50.	Pembekal	Pembekal barangan atau penyedia perkhidmatan.
51.	Pemilik	Pegawai yang didaftarkan sebagai pemilik aset dan dipertanggungjawabkan ke atas aset tersebut.
52.	Pemilik Projek	Individu yang bertanggungjawab terhadap hampir keseluruhan proses kerja projek tersebut. Pemilik projek memainkan peranan utama menentukan keperluan, spesifikasi dan ciri-ciri serahan (produk atau perkhidmatan) yang akan dihasilkan oleh projek tersebut.
53.	Pemilik Proses	Individu yang bertanggungjawab untuk menentukan keperluan bisnes dan mengesahkan sebarang perubahan yang diperlukan berkaitan dengan bisnes proses.
54.	Pengguna	Pengguna terdiri daripada warga JPA dan Pihak Luaran yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT JPA.
55.	Pengurus ICT	Pegawai yang mengetuai organisasi ICT di Jabatan/ Bahagian/ Unit berkaitan ICT.
56.	Pengurus Projek	Individu yang bertanggungjawab untuk merancang dan menguruskan projek dengan baik supaya projek dapat disiapkan mengikut kos, tempoh masa dan kualiti yang telah ditetapkan.
57.	Pentadbir Bangunan	Individu atau entiti yang bertanggungjawab mengurus, menyelenggara, dan mengawasi operasi harian di bangunan JPA.
58.	Pentadbir ICT JPA	Individu atau kumpulan teknikal yang bertanggungjawab mentadbir, mengurus dan menyenggara merangkumi fungsi dan peranan seperti berikut: 1. Pentadbir Rangkaian dan Keselamatan; 2. Pentadbir Pangkalan Data; 3. Pentadbir Portal (Web Master); 4. Pentadbir Pusat Data;

BIL.	ISTILAH	PENERANGAN
		5. Pentadbir Sistem Aplikasi; 6. Pentadbir E-mel; 7. Pentadbir Media Sosial JPA; dan 8. Pegawai Aset ICT.
59.	PTB	Pegawai Tadbir Bahagian
60.	Penyelaras ICT Bahagian	Pegawai Penyelaras ICT merupakan pegawai yang mahir dan berkelayakan mengenai bidang ICT dan dilantik oleh Pengarah Bahagian. Peranan dan tanggungjawab: 1. Perolehan Aset; 2. Penerimaan Aset; 3. Pendaftaran Aset; 4. Penggunaan, Penyimpanan dan Pemeriksaan; 5. Penyelenggaraan; 6. Pelupusan; dan 7. Penyelenggaraan Sistem Aplikasi Teras.
61.	Peralatan Sokongan ICT	Peralatan yang menyokong penggunaan peralatan ICT bagi memastikan kelancaran ICT contohnya projektor, layar, kabel, speaker dan mikrofon.
62.	Perisian	Program atau atur cara komputer yang dapat digunakan dengan sistem komputer tertentu.
63.	Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
64.	Perisian hasad	Perisian hasad (*malware atau malius software*) merujuk kepada pelbagai jenis perisian berniat jahat yang direka untuk mengganggu, merosakkan, atau mendapatkan akses tidak sah kepada sistem komputer dan data.
65.	Pihak Luaran	Pihak Luaran terdiri daripada pembekal, perunding dan pihak-pihak lain yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan atau pelawat yang mengunjungi JPA atas urusan rasmi.
66.	Pihak Berkepentingan	Pihak berkepentingan terdiri daripada pembekal, perunding, pemegang taruh, pelawat dan pihak-pihak lain yang terlibat dalam pengurusan, penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan.

BIL.	ISTILAH	PENERANGAN
67.	Pihak Ketiga	Pembekal, syarikat atau kumpulan syarikat yang dilantik untuk memperbaharui, membekal, menghantar, memasang, mentauliahkan, membangunkan, menguji, dan menyelenggarakan perkakasan atau perisian di JPA.
68.	PKI	*Public-Key Infrastructure* Infrastruktur Kunci Awam
69.	PKP	Pengurusan Kesinambungan Perkhidmatan
70.	PPB	Pasukan Pemulihan Bencana
71.	PSM	Pengurusan Sumber Manusia
72.	Pusat Data JPA	Pusat Data JPA merangkumi dua (2) pengurusan pusat data utama iaitu Pusat Data JPA (BDTM) dan Pusat Data INTAN.
73.	PPL	*Public Key Infrastructure* Infrastuktur Kunci Awam
74.	Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing.
75.	Rahsia Besar	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia.
76.	Rahsia Rasmi	Apa-apa suratan yang dinyatakan dalam Jadual kepada Akta 88 dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi yang boleh dikelaskan sebagai Rahsia Besar/Rahsia/Sulit/Terhad.
77.	*Redundancy*	Kemudahan pemprosesan maklumat yang direka untuk mempunyai saluran atau sumber tambahan untuk menjamin kelangsungan operasi dan mengurangkan risiko kehilangan data atau kecuaian dalam pemprosesan maklumat.
78.	*Restoration*	Pemulihan ke atas data.
79.	*Router*	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.

BIL.	ISTILAH	PENERANGAN
80.	*Screen saver*	Imej yang akan diaktifkan pada komputer setelah ia tidak digunakan dalam jangka masa tertentu.
81.	*Server*	Pelayan
82.	Sistem	Kumpulan dari elemen-elemen yang berinteraksi untuk mencapai suatu tujuan tertentu.
83.	Sulit	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan Kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing.
84.	SLA	*Service Level Aggrement* Perjanjian Tahap Perkhidmatan
85.	SSL	*Secure Socket Layer* Lapisan Soket Selamat
86.	SPA	*Security Posture Assessment* Penilaian Postur Keselamatan
87.	*Switch*	Alat yang boleh menapis (filter) dan memajukan (forward) isyarat paket data antara segmen rangkaian LAN.
88.	TAC	*Transaction Authorisation Code*
89.	Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakkan juga diberi satu tahap perlindungan keselamatan.
90.	*Threat*	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
91.	*Uninterruptible Power Supply* (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan daripada sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
92.	VPN	*Virtual Private Network* Penggunaan Rangkaian Maya
93.	WAN	*Wide Area Network* Rangkaian yang merangkumi kawasan yang luas.

SENARAI LAMPIRAN

LAMPIRAN 1

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER (PKS) JPA

Nama (Huruf Besar): .....

No. Kad Pengenalan: .....

Jawatan: .....

Bahagian (JPA): .....

Organisasi (selain warga JPA): .....

No. Kontrak (jika berkaitan): .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber (PKS) JPA; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan: .....

Tarikh: .....

LAMPIRAN 2

PERAKUAN UNTUK DITANDATANGANI OLEH KOMUNITI KESELAMATAN ATAU MANA-MANA PIHAK LAIN YANG BERURUSAN DENGAN PERKHIDMATAN AWAM ATAU YANG BERKHIDMAT DI KEDIAMAN RASMI KERAJAAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [*AKTA 88*]

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [*Akta 88*] dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi dan suratan rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Saya faham bahawa segala rahsia rasmi dan suratan rasmi yang saya peroleh semasa berurusan dengan perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyatakan atau menyampaikan, sama ada secara lisan, bertulis atau dengan cara elektronik kepada sesiapa jua dalam apa-apa bentuk, sama ada dalam masa atau selepas berurusan dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapatkan kebenaran bertulis daripada pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani satu akuan selanjutnya bagi maksud ini apabila urusan dengan perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia telah selesai.

Tandatangan :

Nama (huruf besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan / Organisasi : .....

Tarikh : .....

Disaksikan oleh

.....

(Tandatangan)

Nama (huruf besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan / Organisasi : .....

Tarikh : .....

Cap Jabatan / Organisasi

Sumber: Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia

LAMPIRAN 3

BIL.	SENARAI PERUNDANGAN DAN PERATURAN
1.	Akta 56 – Akta Keterangan 1950;
2.	Akta 88 – Akta Rahsia Rasmi 1972;
3.	Akta 298 – Kawasan Larangan Tempat Larangan 1959;
4.	Akta 332 – Akta Hak Cipta (Pindaan) Tahun 1997;
5.	Akta 562 – Akta Tandatangan Digital 1997;
6.	Akta 563 – Akta Jenayah Komputer 1997;
7.	Akta 588 – Akta Komunikasi dan Multimedia 1998;
8.	Akta 606 – Akta Cakera Optik 2000;
9.	Akta 629 – Akta Arkib Negara 2003;
10.	Akta Keselamatan Siber 2024 [Akta 854] bertarikh 26 Ogos 2024
11.	Akta 658 – Akta Perdagangan Elektronik 2006;
12.	Akta 680 – Akta Aktiviti Kerajaan Elektronik 2007 (Arahan Teknologi Maklumat 2007);
13.	Akta 709 – Akta Perlindungan Data Peribadi 2010;
14.	Arahan Keselamatan (Semakan dan Pindaan 2017);
15.	Arahan No. 20 (Semakan Semula) – Dasar dan Mekanisme Pengurusan Bencana Negara;
16.	Arahan No. 24 – Dasar dan Mekanisme Pengurusan Krisis Siber Negara;
17.	Dasar Pengurusan Rekod dan Arkib Elektronik;
18.	Etika Penggunaan E-mel dan Internet JPA;
19.	Garis Panduan *IT Outsourcing* Agensi-Agensi Sektor Awam 04/2006;
20.	Garis Panduan Kontrak ICT Bagi Perolehan Perkhidmatan Pembangunan Sistem Aplikasi;
21.	Garis Panduan Pengurusan Rekod;
22.	*Guideline to Determine Information Security Professionals Requirement* for *the CNII Agencies / Organisations;*
23.	*National Cyber Security Policy* (NCSP);
24.	Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”;
25.	Pekeliling Am Bilangan 1 Tahun 2015 – Pelaksanaan Data Terbuka Sektor Awam;
26.	Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022;
27.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan

BIL.	SENARAI PERUNDANGAN DAN PERATURAN
	Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan”;
28.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2015 bertajuk “Pengurusan Laman Web Agensi Sektor Awam”;
29.	Pekeliling Perkhidmatan Bilangan 5 Tahun 2007 bertajuk “Panduan Pengurusan Pejabat bertarikh 30 April 2007”;
30.	Pekeliling Transformasi Pentadbiran Awam Bilangan 3 Tahun 2017: Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan;
31.	Perintah-Perintah Am;
32.	Pelan Pengurusan Pemulihan Bencana JPA;
33.	Penerapan Etika Penggunaan Media Sosial Dalam Sektor Awam (MAMPU);
34.	Polisi Keselamatan Siber (PKS) JDN;
35.	Prosedur Pengurusan Pelaporan Dan Pengendalian Insiden Keselamatan ICT JPA;
36.	Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) versi 1.0 April 2016;
37.	Surat Arahan KPPA Tindakan Ke Atas Penjawat Awam Yang Mendedahkan/ Membocorkan Dokumen/ Maklumat Terperingkat Kerajaan bertarikh 28 Januari 2015;
38.	Surat Arahan MAMPU BDPICT(S) 700-6/1/3 bertarikh 19 November 2009 bertajuk “Penggunaan Media Jaringan Sosial di Sektor Awam”;
39.	Surat Arahan Ketua Pengarah MAMPU Pelaksanaan dan Penggunaan Aplikasi Digital *Document Management System* (DDMS) Sektor Awam yang bertarikh 26 Januari 2015;
40.	Surat Arahan Ketua Pengarah MAMPU - Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam bertarikh 24 Nov 2010;
41.	Surat Arahan Ketua Pengarah MAMPU - Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 dalam Sektor Awam bertarikh 24 Nov 2010; dan Panduan Pelaksanaan Audit Dalam ISMS Sektor Awam (Lampiran kepada Surat Arahan Ketua Pengarah MAMPU);
42.	Surat Arahan Ketua Pengarah MAMPU - Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam bertarikh 22 Jan 2010;
43.	Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
44.	Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;

BIL.	SENARAI PERUNDANGAN DAN PERATURAN
45.	Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network*) Di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;
46.	Surat Pekeliling Am Bilangan 1 Tahun 2025 bertajuk "Garis Panduan Penguruan Kesinambungan Perkhidmatan Dalam Perkhidmatan Awam" *"Business Continuity Management"* (BCM)
47.	Surat Pekeliling Am Bilangan 7 Tahun 2024 bertajuk "Garis Panduan Permohonan Kelulusan Teknikal Dan Pemantauan Projek ICT Agensi Sektor Awam";
48.	Surat Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2015 bertajuk "Panduan Pelaksanaan Program Turun Padang Sektor Awam";
49.	Surat Pekeliling Am Bilangan 3 Tahun 2024 bertajuk "Garis Panduan Pengurusan Risiko Maklumat Sektor Awam";
50.	Surat Pekeliling Am Bilangan 4 Tahun 2024 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam;
51.	Surat Pekeliling Am Bilangan 2/1987 – Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan Akta Rahsia Rasmi (Pindaan 1987);
52.	1Pekeliling Perbendaharaan (1PP) bertarikh 3 Julai 2014: i. Pengurusan Belanjawan (PB); ii. Perolehan Kerajaan (PK); iii. Pengurusan Wang Awam (WP); iv. Pengurusan Aset (KP); v. Pengurusan Kewangan Strategik (PS); vi. Pelaburan Strategik (PA); vii. Pinjaman Perumahan PR);
53.	Akta-akta/ Kaedah/ Pekeliling/ Arahan lain yang berkait.